TECHNICKÁ UNIVERZITA V LIBERCI
Ekonomická fakulta

Zhodnocení rizik a hrozeb spojených s Internetem věcí

Diplomová práce

Studijní program: N6209 – Systémové inženýrství a informatika
Studijní obor: 6209T021 – Manažerská informatika

Autor práce: **Bc. Radek Cihi**
Vedoucí práce: Ing. Petr Weinlich, Ph.D.

Liberec 2019

TECHNICAL UNIVERSITY OF LIBEREC
Faculty of Economics

Evaluation of risks and threats according to the Internet of Things

Master thesis

Study programme: N6209 – System Engineering and Informatics
Study branch: 6209T021 – Managerial Informatics

Author: **Bc. Radek Cihi**
Supervisor: Ing. Petr Weinlich, Ph.D.

Liberec 2019

TECHNICKÁ UNIVERZITA V LIBERCI
Ekonomická fakulta

Akademický rok
2018 / 2019

Zadání diplomové práce

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Radek Cihi**
Osobní číslo:	E17000264
Studijní program:	N6209 Systémové inženýrství a informatika
Studijní obor:	N6209T021 – Manažerská informatika
Zadávající katedra:	katedra informatiky
Vedoucí práce:	Ing. Petr Weinlich, Ph.D.
Konzultant práce:	Ing. Michal Zahradník

Název práce: **Zhodnocení rizik a hrozeb spojených s Internetem věcí**

Zásady pro vypracování:

1. Současná situace v oblasti Internetu věcí.
2. Zhodnocení a srovnání norem platných pro Internet věcí.
3. Analýza rizik Internetu věcí.
4. Vytvoření pravidel pro použití Internetu věcí.
5. Vyhodnocení praktického přínosu v oblasti bezpečnosti Internetu věcí.

Seznam odborné literatury:

BURIAN, Pavel a Graham MEIKLE. 2014. *Internet inteligentních aktivit: models, algorithms, and implementations*. Praha: Grada Publishing. ISBN 978-80-247-5137-5.

BUNZ, Mercedes a Graham MEIKLE. 2017. *The Internet of things*. Malden: Polity. ISBN 978-1509517459.

GUPTA, Aditya. 2017. *IoT Hackers Handbook: An Ultimate Guide to Hacking the Internet of Things and Learning IoT Security. Scotts Valley:* CreateSpace. ISBN 978-1974590124.

HU, Fei a Graham MEIKLE. 2016. *Security and privacy in internet of things (IoTs): models, algorithms, and implementations.* Boca Raton: Polity. ISBN 978-1498723183.

TRIPATHY, B. K a J. ANURADHA. 2018. *Internet of things (IoT): technologies, applications, challenges and solutions*. Boca Raton: Centre national des Lettres. ISBN 978-1138035003.

PROQUEST. 2018. Databáze článků ProQuest [online]. Ann Arbor, MI, USA: ProQuest. [cit. 2018-09-28]. Dostupné z: http://knihovna.tul.cz/

Rozsah práce:	min. 65 normostran
Forma zpracování:	tištěná / elektronická
Datum zadání práce:	1. října 2018
Datum odevzdání práce:	31. srpna 2020

L.S.

prof. Ing. Miroslav Žižka, Ph.D.
děkan Ekonomické fakulty

doc. Ing. Klára Antlová, Ph.D.
vedoucí katedry

V Liberci dne 31. října 2018

Prohlášení

Byl jsem seznámen s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé diplomové práce pro vnitřní potřebu TUL.

Užiji-li diplomovou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Diplomovou práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím mé diplomové práce a konzultantem.

Současně čestně prohlašuji, že texty tištěné verze práce a elektronické verze práce vložené do IS STAG se shodují.

4. 4. 2019

Bc. Radek Cihi

Anotace

Cílem této diplomové práce je zhodnocení rizik a hrozeb spojených s Internetem věcí, které začíná seznámením s technologií, způsobem užití nternetu věcí, dále pokračuje analýzou a vyhodnocením bezpečnostních rizik spojených s touto technologií. První část práce definuje pojem Internet věcí a užití technologie. Další část je úvodem do obecné bezpečnosti a srovnání bezpečnostních norem, které s tím souvisejí. Následuje analýza bezpečnostních rizik, jejich možná obrana v podobě pravidel pro použití internetu věcí a poslední kapitolou je zhodnocení praktického přínosu v tomto odvětví.

Klíčová slova

Bezpečnost, internet, Internet věcí, zásady bezpečnosti

Annotation

Evaluation of risks and threats according to the Internet of Things

Main purpose of diploma thesis is evaluation of risks and threats associated with Internet of Things which starts with introduction with way of using this technology continue with analysis and evaluation of security risks. First part defines the Internet of things and its use. Next part is introduction into general security and comparing current security standards. Followed by analysis of security risks and potential threats. Final chapter contain evaluation and development of rules for the safe using of Internet of things and its contribution.

Key Words

Security, internet, Internet of Things, security principles

Obsah

Seznam zkratek **10**
Seznam tabulek **12**
Seznam obrázků **13**
Úvod **14**
1 Současná situace v oblasti Internet of Things **16**
1.1 Co je to Internet of Things **16**
1.2 Přínos IoT **19**
1.3 Nevýhody IoT **20**
1.4 Použití IoT **21**
1.5 Charakteristika IoT zařízení **23**
1.6 Obecná architektura IoT **24**
1.7 Technické prostředky IoT **26**
1.8 Použité technologie **28**
1.9 Platformy a integrace **34**
2 Zhodnocení a srovnání bezpečnostních norem platných pro Internet věcí **37**
2.1 Bezpečnost IoT **37**
2.2 Standardizační normy **44**
2.3 Společnosti popisující bezpečnost IoT a jeji části **44**
3 Analýza rizik Internetu věcí **55**
3.1 Analýza technických prostředků koncového zařízení **55**
3.2 Analýza technických prostředků poskytovatele služeb **56**
3.3 Celkové řešení IoT **57**
3.4 Definice rizik a způsobů útoku **59**
4 Vytvoření pravidel pro použití internetu věcí **70**
4.1 Ohodnocení pravidel **70**
4.2 Výrobce IoT **71**
4.3 Uživatel IoT **76**
4.4 Mobilní operátor **78**
5 Vyhodnocení praktického přínosu v oblasti bezpečnosti internetu věcí **81**
Závěr **84**
Seznam použité literatury **86**

Seznam příloh 89

Příloha A – Bezpečnostní manuál pro výrobce v tiskové podobě 1/2 90

Příloha B – Bezpečnostní manuál pro výrobce v tiskové podobě 2/2.....91

Příloha C – Bezpečnostní manuál pro uživatele v tiskové podobě.....92

Seznam zkratek

2G	2. generace bezdrátové telefonní sítě
4G	4. generace bezdrátové telefonní sítě
AMQP	Advanced Message Queuing Protocol
AP	Access point
CoAP	Constrained Application Protocol
DDS	Data Distribution Service
EPS	Evolved Packet System
EEA1,2,3	EPS Encryption Algorithm
EEPROM	Electrically Erasable Programmable Read-Only Memory
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Groupe Spécial Mobile
GSMA	Global Systém for Mobile Communications
HD	High Definition
HTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IMEI	International Mobile Equipment Identity
IoT	Internet of Things

LTE	Long Term Evolution
M2M	Machine-to-Machine
MAC	Media Access Control
MMC	Microsoft Management Console
MQTT	Message Queuing Telemetry Transport
NFC	Near Field Communication
NVRAM	Non-Volatiole Random Access Memory
PAN	Personal Area Netowrk
RFID	Radio Frequency Identification
SD	Secure Digital
UMTS	Universal Mobile Telecommunications System
VoIP	Voice over Internet Protocol
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fiber

Seznam tabulek

Tabulka 1 - Architektura IoT, její technologie a standardy..... 54

Seznam obrázků

Obrázek 1 - Propojení Internet of Things 16
Obrázek 2- Obecné schéma Internet of Things 18
Obrázek 3 - Příklad chytré domácnosti 21
Obrázek 4 - Příklad SmartCities 22
Obrázek 5 - 3 vrstvá architektura IoT 24
Obrázek 6 - 5 vrstvá architektura IoT 25
Obrázek 7 - Schéma IoT 28
Obrázek 8 - Platba pomocí technologie NFC 29
Obrázek 9 - RFID čtečka a značka 30
Obrázek 10 - Propojení IoT pomocí technologie Ethernet 32
Obrázek 11 - Použití na mobilních zařízení 34
Obrázek 12 - Apple HomeKit štítek 35
Obrázek 13 - Princip asymetrického šifrování 43
Obrázek 14- Struktura dokumentů GSMA 46
Obrázek 15 - Schéma koncového zařízení 55
Obrázek 16 - Schéma zprostředkovatele služeb 57
Obrázek 17 - Schéma kompletního řešení Internet of Things 58
Obrázek 18 - Příklad SQL Injection 67
Obrázek 19 - Počet zařízení do roku 2025 82

Úvod

Je fenomén dnešní doby. Mnozí si bez něho nedokáží představit život a někteří zase práci. Je jím internet, který za posledních 10 let zažil boom o velikosti 1,8 miliardy připojených uživatelů. Je naším pracovním nástrojem a nejbližším pomocníkem. Spolu se smartphonem tak tvoří nejosobnější zařízení či technologie. (Berners-Lee, 2016)

Historie internetu a jeho počátek je spojen se vznikem počítačů po roce 1945. Příčiny vzniku internetu byly postavené na tehdy počínající studené válce a jeho cíle se zcela lišily od těch současných. Největším podnětem byla potřeba zajištění nezávislé a decentralizovnané komunikační infrastruktury, která i při výpadku některých jejich částí, je schopna nadále fungovat. Internet tak, jak ho známe dnes, dostal podobu až v 90. letech. Právě v této době se dostává mezi širokou veřejnost a slouží lidem mající to štěstí vlastnit domácí počítač. (Anon., 2019)

Diplomová práce je úzce spojena s problematikou využití internetu. Jedná se o Internet of Things – Internet věcí. Internet věcí je označení pro síť fyzických zařízení (vozidel, domácích spotřebičů, smartphonů atd.) s přístupem k internetu. (Bunz a Meikle, 2017) Připojená zařízení využívají internet k tomu, aby si mohla navzájem posílat data a komunikovat interaktivně mezi sebou. Praktickým příkadem může být např. automobil připojený k internetu. Odeslaná data (poloha, stav nádrže, teplota atd.), putující skrz internet do smartphonu propojeného s automobilem. Dalším příkladem IoT může být chytrý termostat. Ten lze ovládat vzdáleně pomocí smartphonu a je tak možné naplánovat, při cestě domů, teplotu v místnosti. (Burian, 2014)

S možnostmi využití IoT vznikají všemožná rizika a způsoby, jak obejít a zneužít bezpečnost ve zmíněných zařízeních a dostat se tak ke koncovému uživateli. V případě chytrého termostatu se nemusí jednat o zásadní bezpečnostní riziko, ale u chytrého automobilu se už může jednat o velký problém. Auto samotné, v rukou třetí osoby, může skončit v lepším případě jen ztrátou dat, ale v tom horším i zneužití kontroly nad vozidlem a možnou nehodou s fatálními následky.

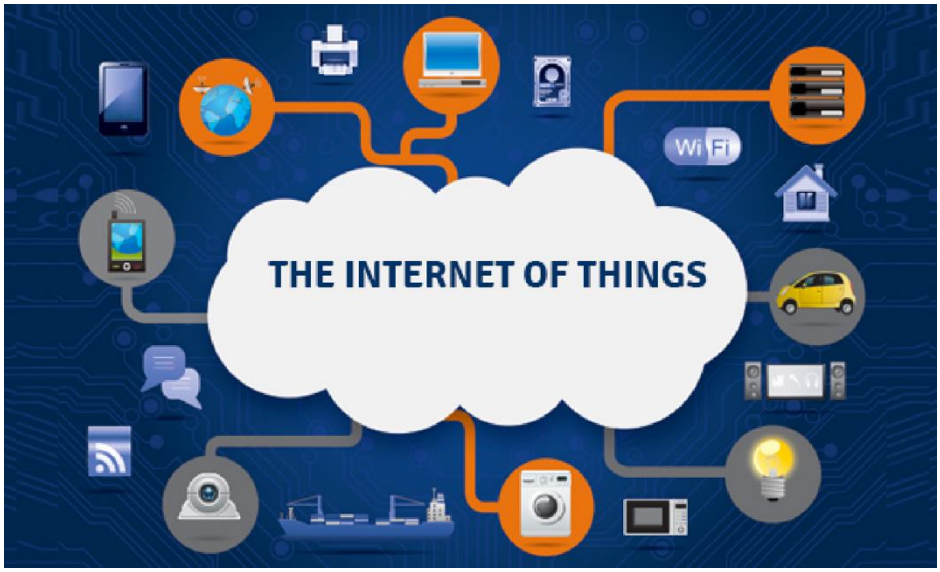
Cílem této diplomové práce je analýza současné situace na poli internetu věcí, zhodnocení jeho technických prostředků, definování této technologie a vyhodnocení její bezpečnosti. Dále pak vytvoření praktického postupu, jak bezpečně Internet věcí používat a také navrhovat. Na závěr je uvedeno praktické použití a přínos tohoto postupu v dané oblasti. Závěrečná práce se snaží pokrýt část tématu bezpečnosti IoT a její obranu. Je „vstupní branou“ do této problematiky a slouží jako materiál pro bezpečnou práci s Internetem věcí.

1 Současná situace v oblasti Internet of Things

V této kapitole se diplomová práce zabývá historií IoT v návaznosti na počátky internetu, popis funčknosti IoT a jeho charakteristika. Dále je uveden způsob komunikace, použití v různých odvětvích, propojení a trendy v IoT. V poslední řadě jsou zmíněny samotní výrobci IoT zařízení.

1.1 Co je to Internet of Things

Termín Internet věcí byl definován v roce 1999 Kevinem Ashtonem, britským technologem, který pracoval s technologií identifikace na základě rádiové frekvence (RFID). Popisuje systém, kde je fyzický svět připojen k internetu prostřednictvím všudypřítomných senzorů, popisující obrázek č.1. Od této doby se stalo IoT diskutovaným tématem na průmyslové a akademické půdě, nicméně stále neexistuje standard modelu, který by IoT popisoval. Při definici IoT je potřeba rozlišovat IoT zařízení a IoT obecně. (Madakam, Ramaswamy, Tripathi, Kheir a Urien, 2015)



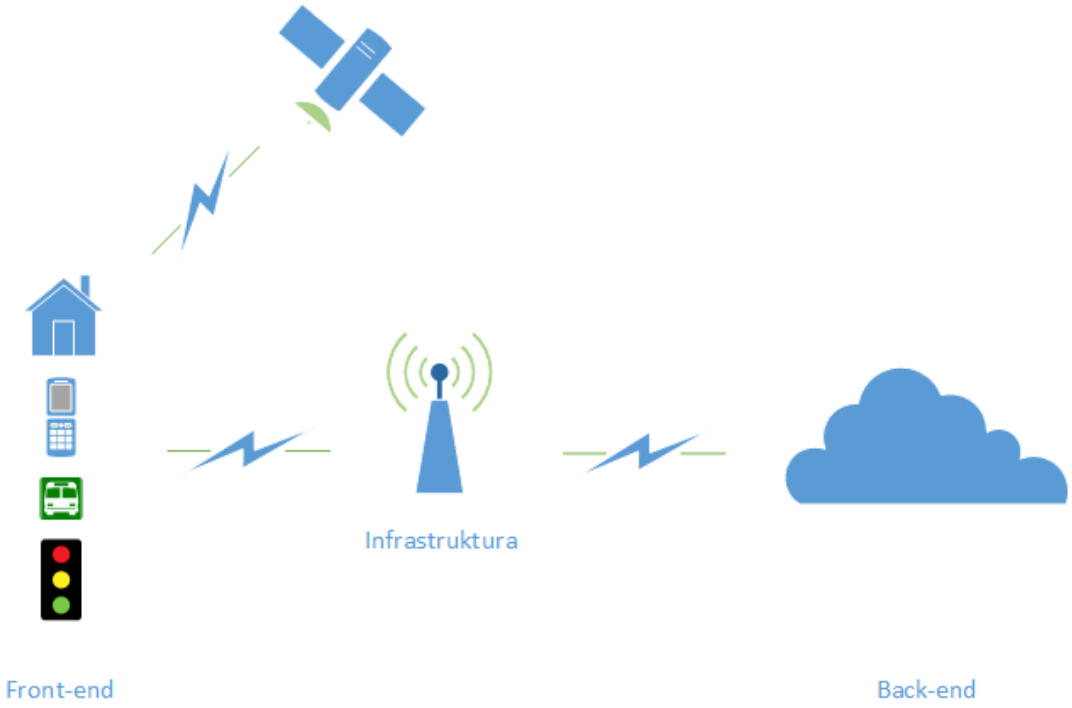
Obrázek 1 - Propojení Internet of Things
Zdroj: https://www.webchoiceonline.com.au/wp-content/uploads/2014/06/internet-of-things-features.png

Institut IEEE je mezinárodní nezisková organizace, usilující o vzestup technologie související s elektrotechnikou. Tento institut popsal IoT obecně jako infrastrukturu propojených objektů připojených k internetu, zaznamenávající a vytvářející data s možností jejich správy. Dále popisují IoT zařízení jako snímač nebo akční člen provádějící specifickou funkci a se schopností komunikovat s jiným zařízením. Je součástí infrastruktury umožňující přenos, ukládání, zpracování a přístup k datům generovanými uživateli nebo jinými systémy. (Madakam, Ramaswamy, Tripathi, Kheir a Urien, 2015)

Od doby, co byl koncept IoT vytvořen, tento trend mění svět na typ informačního systému, kde probíhá neustálé vytváření dat, jejich sběr a vyhodnocení a následné akce s tím spojené. Dnešní technologie a všudypřítomná konektivita má za následek vstup technologií do našeho každodenního života v různých oblastech. (Pathak, 2016) Je to například oblast zdravotní péče, kde se využívají zařízení na dálkové monitorování srdečního tepu pacienta. Další oblastí je domov a jeho automatizace v podobě chytrého termostatu či chytrých zámků. V neposlední řadě to je také v podobě tzv. Smart Cities, v překladu chytrá města, která se snaží automatizovat spoustu rutin a dává tak IoT z daleka největší využití. V nejjednodušší podobě se jedná například o inteligentní zastávky s tabulemi informujícími o odjezdech autobusů a veřejně dostupnou Wi-Fi. Dalším využitím jsou chytrá parkovací místa anebo chytré semafory, které spolu navzájem komunikují a ulehčují tak dopravě. (Dorsemaine, Gaulier, Wary, Kheir a Urien, 2015)

S více než 20 miliardami zařízeními připojených k internetu do roku 2020, jak předpovídájí společnosti Cisco a Ericsson. (Evans, 2011) Svým propojením a dosahem mezi lidmi se dá IoT považovat za budoucnost technologie, která může lidem dělat život příjemnějším a především efektivnějším.

Podle IEET je typický systém IoT tvořen třemi prvky na obrázku č.2. První vrstvou je front-end, kde jsou zařízení se snímací a výpočetní funkcionalitou. Na druhé straně back-end, kde probíhá analýza získaných dat zaslaných prostřednictvím mobilních dat či Wi-Fi přístupových bodů. A mezitím je infrastruktura, která funguje jako prostředek, po kterém putují data mezi front-endem a backe-endem. (Madakam, Ramaswamy, Tripathi, Kheir a Urien, 2015)



Obrázek 2- Obecné schéma Internet of Things
Zdroj: Vlastní

Fron-endové zařízení se liší v různých funkcích a jsou přizpůsobené konkrétnímu úkolu. Většina z nich představuje zařízení s omezeným přístupem k prostředkům a mající velmi omezenou kapacitu, co se týče skladování, komunikace, a dokonce i energie pro ty, která používají jako napájení baterii. Naproti tomu strana back-endu je mnohem výkonnější a tvoří jádro celé myšlenky IoT. S rychlým vývojem cloud computingu je mnoho služeb nasazeno na cloud tak, aby využívaly levné a snadno dostupné úložiště a výpočetní prostředky. Hlavní dodavatelé cloudů, jako jsou Amazon AWS, Microsoft a Google Cloud, poskytují sadu IoT pro urychlení vývoje IoT, kde pomáhají klientům shromažďovat a odesílat data do cloudu, usnadňovat jejich načítání, analýzu a poskytování schopnosti spravovat zařízení. Posledním článkem tohoto schématu je infrastruktura. Je to způsob, jakým se data ze senzorů dostanou ke straně back-endu a obráceně. (Burian, 2014)

1.2 Přínos IoT

Přináši IoT něco nového? Nebo jen to jen hra se slovy a vymyšlení nových technologií? Následující body zachycují některé z podstatných výhod IoT.

Automatizace a řízení – stroje mohou vzájemně komunikovat bez jakéhokoli zásahu člověka, což vede k větší automatizaci a kontrole. Výsledkem bude včasný výstup a rychlejší doba odezvy.

Sběr informací – s IoT je možné zachytit cenné informace prostřednictvím senzorů a pohonů z okolního prostředí.

Čas a peníze – největší výhodou IoT je, že šetří čas a peníze. To je přínosné pro uživatele v jejich každodenním životě, protože zařízení jsou schopna vzájemně komunikovat.

Lepší účinnost – technologie IoT je také efektivní, což produkuje přesnější výsledky. Šetří tím výše zmiňovaný čas a dává tím lidem možnost vykonávat další tvůrčí práci ve svém volném čase.

Lepší kvalita života – tato zařízení mají za cíl poskytnout lepší kvalitu života a pohodlí lidí. (Sannapureddy, 2015)

1.3 Nevýhody IoT

Přestože IoT přináší mnoho příležitostí a výhod, každá mince má své dvě strany, a je tomu tak i zde. IoT má několik nevýhod, které je nutné zmínit.

Kompatibilita – Jelikož zařízení v síti patří různým výrobcům, může dojít k problémům s kompatibilitou. Může to být například problém, kdy se zařízení nemohou připojit k druhému zařízení. Jak bylo zmíněno IoT není nijak zvlášť standardizováno a problém s kompatibilitou by mohla vyřešit právě ona standardizace.

Složitost – IoT je komplexní systém, a proto jsou zde šance na různé případy selhání systému.

Ochrana osobních údajů – problém s ochranou a zachování osobních údajů začíná tehdy, jakmile se jedná o přenos dat mezi více zařízeními, což je v případě IoT samozřejmost. Vznikají zde rizika zneužití osobních údajů.

Pokles v zaměstnanosti – s příchodem technologie, která je schopna nahrazovat lidskou činnost a automatizovat některé procesy, samozřejmě vzniká nedobrovolná nezaměstnanost. Tento fakt může být v blízké budoucnosti problémem.

Technologicky závislý život – není vyloučeno, že s postupem technologie a jejího rozšíření se lidstvo stane více a více závislé. Tato závislost na technologiích a ulehčování některých činností lidstva je spojena také s nižší fyzickou aktivitou, což může mít za následek zdravotní problémy. (Sannapureddy, 2015)

1.4 Použití IoT

Tato kapitola popisuje reálné použití a aplikaci IoT v prostředí domácnosti, životního stylu a také v prostředí průmyslu.

Chytré domácnosti – tzv. Smart Homes je nejdůležitější aplikace IoT. Povědomí lidí o chytrých domácnostech stoupá více a více a jejich ochota kupovat si chytré doplňky roste s nimi. Lidé chtějí, aby jejich domovy byly přeměněny na inteligentní domy, aby mohli vést pohodlnější život. Kdo nechce žít v domě, ve kterém klimatizace nebo topení automaticky reguluje teplotu nebo kde se lampy vypínají tam, kde není požadováno. Produkty chytré domácnosti jsou určeny k šetření času, peněz a energie. Inteligentní domy se brzy stanou běžnou věcí, stejně jako naše smartphony. Příklad chytré domácnosti v praxi je na obrázku č.3.

Obrázek 3 - Příklad chytré domácnosti
Zdroj: https://www.atrium.cz/image/1511/2/inteligentni-dum.jpg

Nositelné chytré doplňky – dnes existuje obrovská poptávka po nositelných zařízeních IoT na trhu. Tyto chytré doplňky obsahují nainstalované senzory a software pro shromažďování dat o chování uživatele. Zařízení často generují velmi užitečné informace pro uživatele a trend je takový, že lidé si tyto informace zamilovávají. Zmíněná zařízení jsou malé velikosti, malého výkonu, ale vysoce efektivní a používají se hlavně pro zdravotní, fitness a zábavné účely.

Vozy připojená k internetu – jedná se o vozy, fungující samostatně prostřednictvím senzorů a připojení k internetu pro komfort cestujících. V této oblasti aktivně pracují velké značky, které už dnes přináší revoluci ve vozidlových systémech.

Průmysl – užití IoT v průmyslu je diskutovaným tématem. Hlavním cílem IoT v průmyslu je umožnit průmyslovým odvětvím se senzory, softwarem a analytikou výstupních dat vyrábět pokročilejší a inteligentnější stroje. Největší výhodou těchto strojů bude kontrola kvality, udržitelnost, sledování zboží a výměna informací v reálném čase. Ožehavým tématem v průmyslu je také automatizace, která v IoT nezná meze.

Inteligentní města – aplikace IoT nejsou omezeny pouze na domovy, ale jsou také použity ve městech. Jak může být město chytré? Prostřednictvím inteligentního sledování, automatizovaného řízení dopravy, správy energie, distribuce vody, monitorování bezpečnosti a životního prostředí. Účelem internetu věcí je vyřešit problémy, kterým obyvatelé měst čelí nejčastěji. Mezi tyto problémy patří například doprava a znečištění okolí. Vizualizace chytrého města na obrázku č.4.

Obrázek 4 - Příklad SmartCities
Zdroj: https://www.passportinc.com/wp-content/uploads/2018/05/shutterstock_578845732-3-1.jpg

Zemědělství – poptávka po zásobování potravinami stoupá, a to zejména kvůli stále rostoucí populaci. Internet věcí má tendenci rozvíjet určité techniky v oblasti zemědělství s cílem zvýšit jejich produktivitu. Kromě toho zemědělci také mohou získávat užitečné informace jako: požadavky na půdu, vlhkost atd.

Energie – inteligentní síťová koncepce získává pozornost po celém světě. Jeho cílem je zlepšit účinnost elektřiny spolu s měřením spotřeby elektrické energie.

Zdravotní péče – inteligentní systémy zdravotní péče jsou schopny shromažďovat zdravotní informace jednotlivce s cílem poskytnout danému pacientovi věrohodnější informace o jeho zdravotním stavu nebo například vystavit zdravotní doporučení. (Burian, 2014)

1.5 Charakteristika IoT zařízení

V kapitole charakteristiky IoT zařízení se jedná o popis vlastností IoT, které jsou pro IoT specifické a dělají z ní právě onu smart technologii.

Inteligence – IoT je kombinace hardwaru a softwaru v souladu s komplexními algoritmy a výpočty. Možnosti IoT plynou právě díky inteligenci, která jim umožňuje reagovat a jednat podle situace a díky tomu i komunikovat s ostatními zařízeními.

Připojení – Jedna z nejdůležitějších vlastností IoT a vlastnost, která dělá z IoT to, čím je. Připojení a tím se myslí nejen připojení k internetu, ale je to také připojení k uživateli, a zejména možnost komunikace směrem k ostatním objektům.

Dynamické vyhodnocování dat – Další vlastností jsou změny a vyhodnocování na základě dynamických proměnných z okolního prostředí, a i změny samotných zařízení vůči vyhodnoceným situacím. Dynamické proměnné mohou být například počasí, místa a čas.

Velikost – Dnes jsou čísla zařízení IoT enormní. Rozmanitost těchto zařízení, což je další z vlastností IoT, z nich dělá mnohem obtížnější technologii na spravování a zpracovávání dat.

Rozmanitost – Jednou z dalších důležitých charakteristik IoT je jejich již zmíněná rozmanitost a heterogenita. Zařízení mají různé hardwarové platformy či prostředky ke komunikaci, a jsou tak schopny komunikovat pomocí různých sítí.

Sběr informací – Senzory jsou důležitou součástí sítě IoT, bez nichž nemohou být změny v prostředí rozlišeny a měřeny. Tyto senzory mají za úkol neustálé zjišťování a sběr dat. Spolu s inteligencí tvoří jeden z nejdůležitějších prvků v IoT. (Hu a Meikle, 2016)

1.6 Obecná architektura IoT

Jak bylo popsáno v předchozí kapitole, IoT je velmi rozmanitou technologií, která obsahuje všemožné kombinace hardwaru, softwaru a způsobu užití. V této kapitole je popsána obecná architektura IoT za použití technologií v praxi tak, aby ji bylo možné lépe pochopit v detailnějším pohledu. IoT není exaktně popsáno a standardizováno, proto je architektura popsána dvěma způsoby popisující její vývoj.

1.6.1 3 vrstvá architektura

Tato architektura byla popisována v začátcích IoT, nicméně v dnešní době je tento model zastaralý a nedostačující. Jedná se však o nejjednodušší způsob rozdělení díky ní lze lépe pochopit vývoj a myšlení v IoT. Zmíněnou architekturu popisuje obrázek č.5. Fyzická vrstva je první úrovní architektury, která zajišťuje hardwarovou část.

Obrázek 5 - 3 vrstvá architektura IoT
Zdroj: https://www.tritonia.fi/download/gradu/7812 (str. 23)

Nachází se zde senzory pro snímání a sběr informací o okolí. Sběr informací probíhá na základě vstupních parametrů či v některých případech na snímání některých objektů. Další vrstvou je úroveň síťová, zajišťující konektivitu k ostatním IoT zařízením, dále také síťová zařízení, která zajišťují přístup k internetu. Tato vrstva má dále za úkol přenášet a vyhodnocovat data. Poslední vrstva zajišťuje předání zpracovaných informací k specifické službě či aplikaci uživateli.

Tato architektura je pro popis IoT nedostatečná, neboť popis by měl obsahovat detailnější pohled na danou problematiku. To je důvod, proč existuje i druhá architektura, rozšířena o 2 další vrstvy a věnuje se jí další kapitola.

1.6.2 5 vrstvá architektura

5 vrstvá architektura je model, který vychází z předchozího modelu, ale liší se ve 3 prvcích. První prvek je tzv. transportní vrstva, zajišťující dopravu dat ze senzorů z fyzické vrstvy. Další je procesní vrstva, která je také známa jako tzv. middleware. Tato vrstva ukládá, analyzuje a zpracovává obrovské množství dat, předáné pomocí transportní vrstvy. Posledním rozdílem je vrstva obchodní, která zodpovídá za celý systém IoT, včetně aplikací, business modelů a také uživatelského soukromí. (Tripathy a Anuradha, 2018)

Obrázek 6 - 5 vrstvá architektura IoT
Zdroj: https://www.tritonia.fi/download/gradu/7812 (str. 23)

1.7 Technické prostředky IoT

V předchozí kapitole je popsána obecná architektura IoT. Tato kapitola na ni navazuje a jsou zde uvedeny jednotlivé vrstvy, jejich obecný popis technologie a jejich použití v jednotlivých vrstvách.

Fyzická vrstva je první při popisu architektury IoT. Jak už bylo zmíněno, tato vrstva má na starost sběr dat pomocí senzorů. Těchto senzorů je v praxi obrovský počet, proto bude v diplomové práci popsáno zařízení, které má k člověku nejblíže. Tím zařízením je smartphone. Smartphone má senzorů hned několik, je to například senzor polohy (GPS), senzor pohybu (gyroskop, akcelerometr), senzor okolního prostředí (fotoaparát), senzor světla, mikrofon a mnoho dalších. Jsou to senzory hojně využívány různými aplikacemi v zařízení a poskytují velmi zajímavé informace i v případě využití více senzorů na jednou. Jako příklad lze uvést fotoaparát se senzorem polohy, kdy se k fotografii přidají data o GPS poloze.

Další senzory, použité mimo oblast smartphonu, jsou například: teplotní senzor, senzor tlaku, vlhkosti či různá zdravotní data (krevní cukr, tep atp.). (Tripathy a Anuradha, 2018)

Transportní vrstvu lze také nazvat vrstvou komunikační. IoT pro komunikaci používají různou sadu protokolů a standardů. Dělí se přitom dle rozsahu na: zařízení s malým rozsahem a nízkou energetickou náročností a zařízení s rozsahem středním.

Nejběžnějšími komunikačními technologiemi pro zařízení s nízkou energetickou náročností a krátkým rozsahem jsou RFID a NFC. Pro zařízení s rozsahem středním jsou to technologie Bluetooth, ZigBee a WiFi. Důležitým prvkem této vrstvy je také MAC adresa, což je identifikátor zařízení v sítí. (Tripathy a Anuradha, 2018)

Procesní vrstva je spojená se zpracováním doručených dat z transportní vrstvy. Zpracování dat probíhá na softwarové úrovni. Existují zde 2 typy softwarových řešení: middleware a samotné aplikace.

Komponenta middleware je určena programátorům a vytváří abstraktní náhled hardwaru. Jejím hlavním úkolem je zajištění schopnosti vzájemné spolupráce různých

systémů při komunikaci, poskytování vzájemných služeb a dosažení jejich součinnosti. Mezi tato řešení patří například OpenIoT, MiddleWhere, Hydra, FiWare nebo Oracle Fusion Middleware. (Singh, 2015) Formátování dat a jejich prezentace je úkol vrstvy aplikační. V prostředí internetu existuje protokol HTTP, který má za úkol přenos hypertextových dokumentů. V IoT je tento protokol nevhodný a je zde použito protokolů hned několik. Mezi nejrozšířenější patří CoAP, MQTT, AMQP a DDS. (Tripathy a Anuradha, 2018)

Obchodní vrstva slouží výrobcům k vyhodnocování dat pro jejich potřeby. Data uložená na cloudech, důkladně analyzována a vyhodnocována pro další vývoj daného zařízení. Vyloučit se nedá ani obchod s danými daty. (Tripathy a Anuradha, 2018)

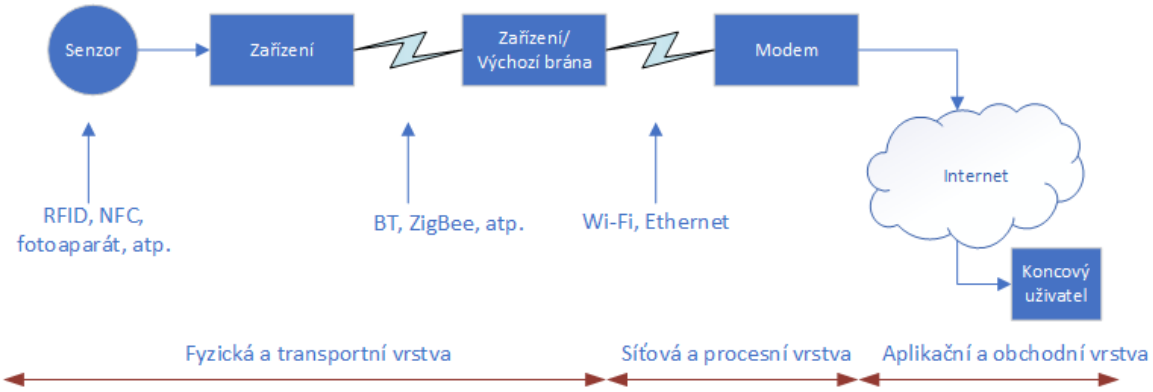
V předchozích odstavcích byly popsány jednotlivé vrstvy modelu IoT. Je velmi důležité zmínit, že komunikace mezi těmito vrstvami neprobíhá jednosměrně. Technologie IoT si totiž žádá, aby komunikace probíhala obousměrně.

Přestože v IoT existuje spoustu rozmanitých zařízení, všechna zařízení mají jedno společné. A tím je fakt, že zařízení vycházejí z modelu 5 vrstev. Obecně tedy platí, že IoT by mělo obsahovat 5 základních rysů:

1. Senzory
2. Výchozí brána
3. Komunikační síť
4. Software pro zpracování dat
5. Koncová aplikace

1.8 Použité technologie

V předchozí kapitole byly popsány technické prostředky IoT z abstraktního pohledu vrstev a okrajově byly zmíněny technologie, které jsou v každé vrstvě použity. V této kapitole jsou zmíněné technologie detailněji popsány a vsunuty do kompletního řešení s vysvětlením a uvedení praktických příkladů. K tomu bude sloužit Obrázek č.7.



Obrázek 7 - Schéma IoT
Zdroj: https://www.tritonia.fi/download/gradu/7812 (str.14)

Počátkem je fyzická vrstva a transportní vrstva, které řeší problematiku sběru dat ze zařízení ze senzorů. Z těchto senzorů a technologií pro přenos dat stojí za zmínku technologie NFC, RFID, Bluetooth a ZigBee.

Zkratka NFC stojí za „Near Field Communication“. V překladu se jedná o „blízkou komunikaci“. Tato technologie je velmi podobná technologii RFID, nicméně na rozdíl od RFID, NFC je bezdrátovou komunikací s krátkým dosahem a vysokou frekvencí, která umožnuje bezkontaktní přenos dat mezi elektronickými zařízeními ve vzdálenosti 10 cm. V rychlosti přenosu si vybírá mezi rychlostí 106kbps, 212kbps anebo 424kbps. Je to technologie, která je také velmi podobná BT. Avšak rozdílem je právě vzdálenost 10 cm. Mezi další rozdílný prvek pak lze zařadit nepovinné párování dvou zařízení u NFC technologie a dochází tak k zjednodušení procedury autorizace. V současné době NFC obsahuje většina mobilních zařízení. (Tripathy a Anuradha, 2018)

Příklady aplikace NFC:

1. **Přístupová práva** – kdy se mobilní zařízení stává klíčem. V praxi je to nahráný kód v mobilním telefonu a jeho následné použití u chytrých dveří obsahující NFC čtečku s databází povolených kódů.
2. **Platba** – kdy uživatel použije zařízení jako peněženku. Což znamená kreditní kartu s podporou NFC anebo opět mobilní telefon, který je spárován s mobilní bankou. Příklad placení pomocí NFC je znázorněno na obrázku č.8.
3. **Připojení** – případ, kdy je NFC technologie použita k „párování“ dvou zařízení a je zajištěn následný přenos dat.
4. **Prozkoumávání** – uživatel může po přiložení k zařízením získat různá data. V praxi je to podobné QR kódům s tím rozdílem, že není použit fotoaparát, ale NFC čtečka. (Mengdi, 2016)

Obrázek 8 - Platba pomocí technologie NFC
Zdroj: https://fitsmallbusiness.com/wp-content/uploads/2018/05/word-image-499-1024x576.png

Další technologií je tzv. RFID, což je zkratka „Radio Frequency Identification“. Je to bezdrátová technologie umožňující rádiovým signálům identifikovat konkrétní cíl, číst

a zapisovat související data bez vytvoření mechanického či optického kontaktu mezi systémem a zařízením. V RFID se rozlišují dvě role: **značka** a **čtečka** (viz. Obrázek č.9). Čtečka vyšle rádiové signály, které používají frekvenční elektromagnetická pole. Tato pole je možné pomocí značky pohltit a „nabít se tím“. Vyšle tak signál zpět směrem ke čtečce, aby se automaticky identifikoval. Tyto značky získávají energii z čtecích elektromagnetických polí, takže nepotřebují baterii. Využití technologie RFID má několik výhod.

1. **Snadné čtení** – v RFID není potřeba zdroje světla, čtení probíhá za vyslání radiových vln. Pokud má značka vlastní baterii, rozpoznávání může být až ve vzdálenosti 30 metrů.
2. **Rychlý reakční čas** – když je značka v dosahu elektromagnetického pole, čtecí zařízení ji může okamžitě identifikovat a číst informace.
3. **Dlouhou životnost** – čtečka jako taková může být použita i v znečištěném prostředí.
4. **Komunikace v reálném čase** – značka a čtečka mohou komunikovat v rozsahu 50 až 100krát za sekundu. (Mengdi, 2016)

Obrázek 9 - RFID čtečka a značka
Zdroj: https://www.gme.cz/data/product/1024_1024/pctdetail.774-011.1.jpg

Vzhledem k výše zmíněným skutečnostem je technologie RFID použita hlavně v průmyslovém odvětví.

Ze senzorů a technologií, které pořizují data se diplomová práce dostává k technologiím, zpřístupňující komunikaci mezi dalšími zařízeními. Těmito technologiemi jsou Bluetooth a ZigBee.

Bluetooth je bezdrátová technologie, umožňující výměnu dat na krátkou vzdálenost. Používá k tomu vysokofrekvenční rádiové vlny. Aby zařízení bylo možné uskutečnit komunikaci s bluetooth technologií (např. sluchátka či hodinky) musí obsahovat počítačový čip, přijímač a software, podporující konektivitu bluetooth. Pro úspěšnou komunikaci je nejprve provedena autorizace. Poté je vytvořena dočasná síť krátkého dosahu. Tuto síť je možné vytvořit až z 8 zařízení, přičemž jedno ze zařízení má roli „master" a všichni ostatní roli „slave". V současné době existují dva hlavní typy technologie bluetooth. Prvním typem je technologie s názvem „Bluetooth Basic Rate/Enhanced Data Rade", jenž se používá především v typu připojení, kde je potřeba vysokého datového toku a není kladen důraz na spotřebu. Druhým typem je „Bluetooth-Low Energy", použitý především v chytrých domácnostech.

Poslední technologií, která uzavírá fyzickou a transportní vrstvu je tzv. ZigBee. Je to protokol postavený na IEEE802.15.4 standardu, což znamená, že se jedná o nízkoenergetickou síť LAN, která je na frekvenci 2.4Ghz. (Mengdi, 2016)

Tato technologie má několik vlastností:

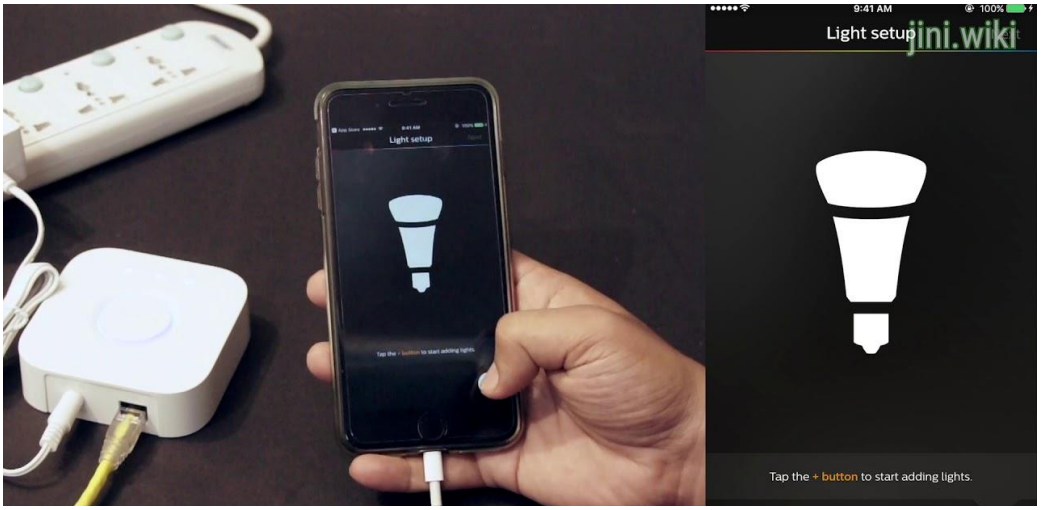
1. **Nízká spotřeba energie** – ZigBee podporuje tzv. úsporný režim, který při napájení 2x AA baterií dokáže vydržet 6 až 24 měsíců. V porovnání s WiFi či BT je tato technologie velmi energeticky úsporná.
2. **Nízká přenosová rychlost** – protokol podporuje maximální přenosovou rychlost 250kbps.
3. **Krátký rozsah přenosu dat** – rozsah přenosu dat je obecně mezi 10 až 100 metry.
4. **Rychlá odezva** – odezva a probuzení z výše zmíněného úsporného režime je pouze 15ms. Připojení uzlu k síti trvá 30ms.
5. **Vysoká kapacita uzlů** – Možnost správy až 65 000 uzlů.

V dnešní době se ZigBee používá hlavně v bezdrátových tzv. M2M sítích a jeho použití mezi spotřebiteli bývá velmi časté. (Mengdi, 2016)

V předchozích vrstvách šlo o propojení mezi zařízeními IoT a výměnu jejich dat. Předmětem síťové a procesní vrstvy je v zjednodušené podobě propojení s vnějším světem, tedy s internetem. K tomu slouží technologie WiFi, mobilní data a kabelové připojení Ethernet.

WLAN, nebo také Wi-Fi, je technologie založená na standardu IEEE 802.11.(Burian, 2014) Jedná se o bezdrátovou síť, umožňující připojení a zpřístupnění internetu dvou a více mobilních zařízení. Toto připojení je založena na tzv. AP (Access Point), což lze z angličtiny přeložit jako přístupový bod, ke kterému se připojí zařízení a v jehož rozmezí pokrytí mají přístup k internetu. V současné době je to standard, využitý ze všech nejvíce, a povědomí o něm má téměř každý. Wi-Fi podporuje vysoký datový tok a větší vzdálenost oproti např. BT. Ovšem tato podpora je vykoupena faktem, že připojení Wi-Fi není vhodné pro zařízení s nízkým napájením. (Singh, 2015)

Nejvhodnější technologií z hlediska dosahu, je technologie mobilních dat. Pokrytí mobilních dat je takřka všude, díky kumuninakční infrastruktuře vybudované nadnárodními společnostmi. Mobilní data jsou kategorizována dle rychlosti připojení. Nejvyužívanější jsou dnes tzv. 3G, H+ a 4G sítě, kde se rychlost přenosu dat pohybuje až k 100 Mbps. Nicméně, vše má svou dobrou i špatnou stránku. Všudypřítomný, rychlý a stabilní signál je vykoupen měsíčními náklady a vysokou spotřebou baterie v zařízení, které tato mobilní data využívá. Pro tyto důvody se mobilní data ve spojení s IoT používají



Obrázek 10 - Propojení IoT pomocí technologie Ethernet
Zdroj: https://i.ytimg.com/vi/9y9jpq5bVBI/maxresdefault.jpg

v průmyslové sféře. Ukázku připojení ethernet lze vidět na obrázku č.10. (Tripathy a Anuradha, 2018). Od získaných dat ze senzorů po jejich „cestu“ přes zařízení, internet, až k výrobci a spotřebiteli. Cílová rovinka, která je nazvána jako aplikační a obchodní vrstva. Hlavní cíl v této práci bude hlavním předmětem bezpečnosti, neboť v těchto vrstvách probíhá komunikace se světem. Jak už bylo zmíněno, aplikační vrstva obsahuje sadu protokolů, které se starají o komunikaci a „zapouzdření“ dat. Jako hlavní protokoly jsou zmíněny CoAP, MQTT, AMQP a DDS. (Asim, 2017)

Protokol CoAP je alternativa HTTP a je použit ve většině IoT zařízeních. Používá tzv. EXI, což je datový formát, vycházející z XML jako tomu je u HTML, ale je daleko efektivnější. Přenos dat je řešen za použití protokolu UDP. Protokol se používá u zařízení v kombinaci tzv. one-to-one. TCP a HTTP totiž vyžadují autorizační proces tzv. „three way handshake“ a další složité mechanismy. Proto je CoAP vhodný pro zařízení s nízkou spotřebou energie a je tak rozšířený v IoT. Zatímco CoAP používá pro přenos dat UDP, protokol MQTT používá pro přenos protokol TCP. Použití tohoto protokolu je v kombinaci tzv. many-to-many. Znamená to přenos zpráv mezi více klienty. Dalším protokolem je protokol DDS, který se využívá v komunikaci machine-to-machine. Je to protokol, který umožňuje real-time výměnu informací. V obchodní vrstvě jsou to pak řešení, která ukládají a vyhodnocují data. Těmto řešením se říká tzv. Cloud Computing, což je internetová služba, umožňující uživatelům uložit a analyzovat data ze senzorů. Nevyžaduje to tak žádný prostor v síti či v počítači a díky řešení cloudu, jsou data rychleji zpracovány. Princip cloudu je, že uživatel nemusí znát polohu, ale spojení skupiny počítačů se tváří jako jeden přístupný bod, který je dostupný kdykoliv na libovolném místě. Jediné, co je potřeba je připojení k internetu. (Asim, 2017)

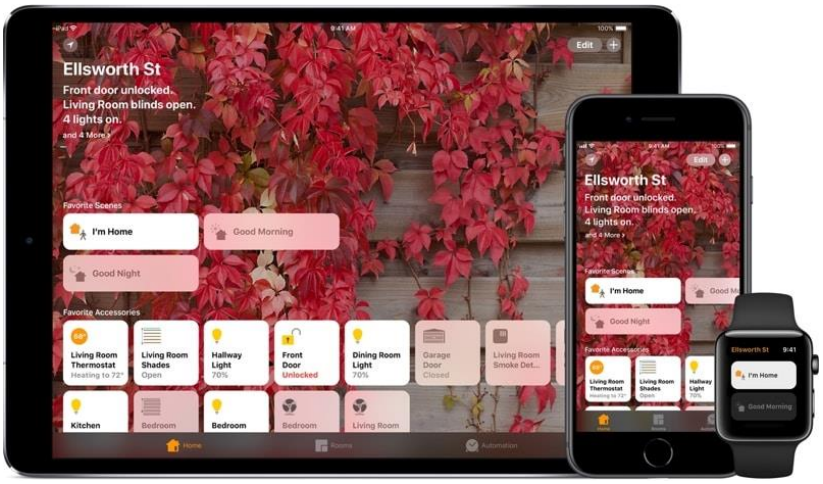
Architektura Cloud Computingu se skládá ze tří služeb:

1. **Infrastruktura jako služba** – nabídka uložiště a výpočetního výkonu jako službu konečnému uživateli.
2. **Platforma jako služba** – nabídka kompletní platformy včetně softwaru po dobu životního cyklu.
3. **Software jako služba** – nabídka licencovaného softwaru jako služba pronajímaná uživateli. (Burian, 2014)

1.9 Platformy a integrace

V předchozích kapitolách je seznámení s IoT vysvětlení základních funkcí, softwarového pozadí a přiblížení architektury pomocí vrstev. V předchozích kapitolách bylo zmíněno, že IoT je nestandardizované paradigma a aby zařízení mohlo spadat pod trend IoT, tak k výrobě stačí pouze dané zařízení připojit k internetu. Pro tento případ vznikly tzv. platformy, které standardizují, jakým způsobem spolu zařízení komunikují a usnadňují tím implementaci a pozdější rozšíření sítě. Tyto kapitoly lze rozdělit podle užití, a to buď v domácím či výrobním prostředí.

Nejznámější platformy v domácím užití jsou od výrobců Apple (příklad na obrázku č.11), Google a méně známější firma Nest. Tyto firmy jsou nejznámější právě kvůli prodejnosti jejich smartphonů a rozdělení podílu trhu. Za systém iOS je to samozřejmě Apple s tzv. Apple HomeKit, za systém Android jsou to Google se svým Google Home a platforma Nest, která je multiplatformní. (Rogers, 2014)



Obrázek 11 - Použití na mobilních zařízení
Zdroj: https://securitybaron.com/blog/home-automation-platforms-apple-homekit-vs-amazon-alexa-vs-google-home/

V prostředí domácnosti, tyto platformy mají za úkol, co nejvíce ulehčit uživateli integraci chytrých zařízení a správu pomocí smartphonu. Největší tržní podíl v tomto odvětví má Apple se svým HomeKitem. Apple byl také první, který se ze všech výrobců mobilních zařízení začal zajímat o IoT. (Rogers, 2014) Tato platforma nenabízí jen pouhé připojení do ekosystému Apple, ale také silnou stránkou této platformy je automatizace některých procesů. Může to být například proces, kdy při odjezdu z práce domů se zapne chytrý termostat.

Obrázek 12 - Apple HomeKit štítek
Zdroj: https://www.forbes.com/sites/brucerogers/2014/07/08/apple-and-google-dominate-internet-of-things-influence-with-home-automation-efforts

Produkty, které podporují Apple HomeKit jsou označeny štítkem na obrázku č.12 a zároveň se štítkem s osmistým číslem ve tvaru XXX-XX-XXX, které slouží jako identifikátor v síti. Nutno zmínit, že tato označení je možné použít až poté, co zařízení projde schvalovacím procesem od Apple, jelikož HomeKit je uzavřená platforma. (Rogers, 2014)

Platforma od konkurenční společnosti Google nabízí to samé, co Apple. Z pohledu konkurence je to taky vyžadováno, neboť si ani jedna z firem nemůže dovolit nebýt konkurence schopná. U uživatelů androidu je to tedy aplikace integrovaná přímo v Android smartphonu a možnost její komunikace s IoT zařízeními. Bohužel, společnost Nest je v tomto pohledu v nesnadné pozici, protože pro svá zařízení musí mít zvlášť aplikaci, která poté komunikuje s Nest zařízeními. V prostředí průmyslu jsou to poté platformy od společností jako IBM, Amazon či Google. V porovnání s domácím použití se jedná v principu o to samé. Úkolem těchto platforem je co nejjednodušší integrace, správa a následná analýza dat. S tím rozdílem, že v prostředí průmyslu se jedná o mnohonásobně větší počet senzorů a s tím také mnohonásobně větší objem nasbíraných dat. Samozřejmostí je rozdílnost zpracování dat, neboť každé odvětví má rozdílné cíle. (Carter, 2015)

Tato kapitola uzavírá kompletní část současné situace v IoT. V úvodu byla popsána základní funkčnost IoT, její přínosy a nevýhody s následnými příklady použití. Další částí byla jeho obecná charakteristika s architekturou. V následující kapitole se poté architektura a její funkčnost převedla na reálné příklady použití. V závěru této části byl nastíněn trend platforem, které v současné situaci v IoT existují. Tato kapitola slouží jako vstupní brána do problematiky IoT a je nezbytná k dalšímu čtení této diplomové práce. Následující kapitola slouží jako úvod do problematiky IT a IoT bezpečnosti.

2 Zhodnocení a srovnání bezpečnostních norem platných pro Internet věcí

Tato kapitola slouží jako úvod do bezpečnosti IoT. Má za úkol seznámit čtenáře s obecnou bezpečností IoT, srovnání platných bezpečnostních norem a slouží hlavně jako teoretický úvod do dalších kapitol.

2.1 Bezpečnost IoT

Před několika lety prohlásila organizace Spojených národů, že internet je základním lidským právem a že všichni lidé na celém světě by měli mít přístup k širokopásmovým službám. Nedávno byly v zemích, jako je Francie, Řecko, Španělsko a další přijaty zákony, aby byl přístup k internetu široce dostupný anebo aby se zabránilo tomu, že stát nepřiměřeně omezí přístup jednotlivců k informacím a internetu. (Velocci, 2016)

Tato prohlášení jsou výsledkem rychlých sociálních a technologických změn, které vyplynuly z růstu internetu. Výsledkem toho je, že se internet stává způsobem života, jedním z hlavních zdrojů všech druhů informací a nejběžnější metodou pro udržení propojení s blízkými a vrstevníky. Internet není jen technologií, stal se součástí nás.

Již více než deset let se zájem o všudypřítomný přístup k informacím zvýšil. V tomto okamžiku se náklady na komponenty prudce snížily, zatímco přístup k bezdrátovým službám a rychlost těchto služeb se dramaticky zvýšil. Protokoly, životnost baterie, a dokonce i obchodní modely se vyvinuly tak, aby vyhovovaly stále rostoucí poptávce po informacích a konektivitě.

A takto by se Internet věcí dal chápat v jeho elementární podobě. Ve skutečnosti se nejedná o zmíněné věci, ale zaobírá se především lidmi, a proto je možné ho chápat jako internet lidí či internet nás samotných. Lidský život je každým rokem více a více propojen se světem digitálním či se světem internetovým. A z toho důvodu je nezbytně nutné chránit lidský fyzický svět před digitálními hrozbami, tak aby byla udržena jeho bezpečnost. Internet věcí je skvělá příležitost pro svět, aby se mohl posunout kupředu, aby vytvářel stále větší databáze

znalostí, sdílených zkušeností a výbuchů inovací. Aby však tato technologie fungovala efektivně, musí být zajištěny technologie, které řídí tuto konektivitu. Musí prosazovat soukromí, spolehlivost a kvalitu služeb nezbytných k tomu, aby tato velkolepá utilita, tato nezbytná základní potřeba byla k dispozici všem, kteří to vyžadují.

Aby se Internet věcí efektivně vyvíjel, musí se vyřešit bezpečnostní problémy spojené s jeho růstem. Soukromí a bezpečnost dat uživatelů, resp. zákazníků, je největší výzvou pro internetovou bezpečnost. V případě IoT tomu není jinak a s počtem zařízení v domácnosti je to dokonce mnohem důležitější. S tímto je spojeno několik výzev, se kterými se potýkají výrobci.

- **Dostupnost** – zajištění nepřetržité konektivity mezi koncovými body a jejich příslušnými službami.

- **Identita** – ověření koncových bodů, služeb a zákazníka nebo koncového uživatele, který obsluhuje koncový bod.

- **Ochrana osobních údajů** – snížení možnosti ohrožení jednotlivých koncových uživatelů.

- **Zabezpečení** – zajistit, aby mohla být celistvost systému ověřována, dostihnutelná a sledována. (Hu a Meikle, 2016)

A další s tím spojené jsou druhy ohrožení, které z těchto výzev plynou. V IoT tak můžeme rozlišit 4 druhy ohrožení:

- **Krádež** – tato skupina ohrožení se týká především domácností a způsobu, jakým jsou „ochráněny“. Jestliže se jedná např. o dveře s chytrým zámkem, či vzdálené ovládání vrat od garáže. V obou případech jde o způsob průniku do budovy a vyústění ke způsobené škodě.

- **Soukromí** – v případě průniku do cloudů, kde jsou uložena citlivá data např. biometrická data, informace o zdraví, GPS souřadnice nebo uložená hesla uživatelů. V tomto případě se jedná o jeden z nejzávažnějších druhů ohrožení.

- **Bezpečnost** – rozšíření IoT do automobilů a osobních zařízení jako např. do chytrých hodinek může způsobit i újmu danému uživateli. Větším měřítkem může být například omezení infrastruktury ve městech a zneužití ovládání např. elektřiny, dopravních světel či vodovodních systémů.

- **Produktivita** – v této kategorii může ohrožení způsobit újmu v produktivitě práce. Např. zneužití výrobní linky, navigačních systémů apod. (Hu a Meikle, 2016)

Příkladem takové hrozby je případ z roku 2016, kdy bylo použito 145 tisíc IoT zařízení k tzv. DDOS útokům. Díky počtu zařízení se tyto útoky řadí mezi nejsilnější útoky vůbec a jejich použití je zdaleka nejjednodušší. (Goodin, 2016)

Další příklad průniku do systému byl zaznamenán v roce 2015, kdy dvojice Charlie Miller a Chris Valasek pronikla do automobilu připojeného k internetu a dokázala vzdáleně kontrolovat některé z jeho funkčností. Dvojice dokázala zvyšovat či snižovat rychlost vozidla, vypnout či zapnout rádio a dokázala dokonce vozidlo zastavit. Tento odstrašující příklad ukazuje, jak moc velké nebezpečí z možnosti připojení zařízení k internetu plyne. Kdyby se nejednalo pouze o dvojici zvídavých nadšenců, mohla by tato situace skončit tragicky. (Gelles, Tabuchi a Dolan, 2015)

Je otázkou, jaké jsou příčiny výše zmíněných případů. Nicméně v obecném pojetí můžeme říci, že příčinou je především rozmanitost zařízení IoT, rychlý vzestup nových zařízení na trhu výrobců při nedostatečném kladení důrazu na bezpečnost. V současné době neexistuje žádný jednotný standard, který by komplexně popisoval případné útoky IoT nebo zranitelnost a způsoby, jak se těmto útokům vyhnout. Nicméně existují zde standardy nepřímo související s IoT a ty jsou popsány v nadcházejících kapitolách.

2.1.1 Hesla

V dnešní době jsou hesla používána jako obecný prostředek k ověřování totožnosti uživatele. Uživatel je legitimován za oprávněného k přístupu tehdy, kdy prokáže znalost hesla. Bezpečnost tohoto procesu, který se na zývá autentifikace, závisí na síle hesla, jeho zabezpečení ze strany uživatele a následně ze strany serveru, ověřující heslo. Následující odstavce představují několik možných forem autentizace a volbu hesel.

Výzkumníci z National Taiwan ocean University a Tchaj-wan Institute of Science navhrují, že se uživatelé prokáží bez použití hesla. Namísto potřeby neustálého zadávání kombinací přihlašovacích jmén a hesel přisli s nápadem, kdy se stačí úspěšně ověřit ze strany serveru a toto schéma ověření je následně komunikováno skrze platformy. Cílem tohoto výzkumu bylo potvrzení myšlenky, že jedno kompletní přihlášení změnší počet útoků namísto opakovaného přihlašování se. Samotné útoky jsou závislé na získání přihlašováacího údaje, kterým je jméno a validní heslo. (Bachmann, 2014)

Další forma ověření, v dnešní době velmi oblíbená a také zavedena, je ověření za použití biometrických údajů. Uživatel a jeho unikátní vlastnosti (také jako biometrické údaje) jako otisk prstů či oční sítnice jsou uloženy jako digitální hash a při přihlašování jsou tyto hashe porovnávány na stejném principu jako klasické přihlašovací údaje a následně vyhodnoceny jako shodné či nikoliv. V dnešní době, kdy je více a více mobilních telefonů, podporující otisky prstů či snímání očních sítnic se tato forma autentizace stává čím dal tím rozšířenější.

Výzkumníci ze skupiny DARPA také zkoumají dynamiku úderů uživatele a za pomocí této metriky ho následně rozpoznávají. Každý uživatel podel DARPA má totiž svůj rytmus a styl psaní na klávesnici a mohou tak přesně a bezpečně identifikovat jednotlivého uživatele. Uživatel je rozpoznán na základě jedinečného vzoru a následně mu je udělen přístup bez požadavku na poskytnutí přihlašovacích informací.

Od 90. let výzkumníci zkoumali myšlenku používání vizuálních hesel. Teorie, ve které se používají obrázky na rozdíl od textu, je považována za bezpečnější a lépe zapamatovatelnou. Princip použití této formy autentizace je na základě výběru uživatele. Uživatel si při registraci vybere ze souboru několika obrázků a celkově tento výběr

tvoří jeho ověřovací klíč. Jeden z nejpopulárnější vyhledávacích systémů je tzv. PicturePassword.

Zatímco formy autentizace jako heslo na jedno použití, biometrické ověření či bizální hesla se zdají být pravděpodobná, existují návrhy, které jsou více než podivné. Mezi tyto formy patří např. nápad použití elektronické tetování nebo elektronické pilulky. (Bachmann, 2014) Tyto formy by sloužily taktéž jako náhrada hesla, nicméně použití v případě elektronické pilulky je více než nepravděpodobné. Každopádně zde existují tací, kteří mají opačný názor a na vývoji těchto forem již pracují výzkumníci z týmu Advanced Technology společnosti Motorola. Společnost Motorola také nedávno debutovala s implementováním plošného spoje do paže jako forma tetování. Společně s tetováním společnost Motorola také vyvíjí formu autentizace, kterou nazývá „vitamin authentication“. V případě anglického překladu by se jednalo o autentizace pomocí vitamínů, nicméně je to výše zmíněný princip pilulek. Tato technologie spočívá v polykání drobných senzorů uživatelem. Tyto senzory jsou pojmenovány jako zdravotnický prostředek a s pomocí kyseliny v žaludku jsou poháněny. Je to vskutku revoluční nápad, který by změnil tělo na autentizační prvek. (Singh, 2015)

2.1.2 Kryptografie

Kryptografie je základním kamenem bezpečnosti v IoT. Je implementována jak za pomocí hardwarových, tak i softwarových technologií. Kryptografie je věda šifrování a dešifrování datové komunikace za účelem ochrany informací. Existují tři hlavní funkce kryptografie:

- **Důvěrnost** – zabraňuje získávání citlivých informací neoprávněným uživatelem nebo zařízením a současně zajistí, že byl přijat správným uživatelem nebo zařízením. Šifrování dat je často používanou metodou zajištění důvěrnosti. Obvyklým příkladem je Transport Layer Security (TLS), která byla dříve protokolem Secure Sockets Layer (SSL), bezpečnostním protokolem pro komunikaci odesílanou přes internet a kompatibilní s velkým počtem internetových protokolů.
- **Integrita** – integrita zahrnuje zachování konzistence, přesnosti a důvěryhodnosti údajů v průběhu celého životního cyklu. Obvyklou metodou ochrany integrity dat je

vytvoření tzv. hashe (kryptografické znázornění) přijatých dat a porovnat je s hashem původní zprávy.

- **Autentizace** – proces, který potvrzuje identitu vzdáleného zařízení nebo zařízení v síti. Tento proces zajistí, že do sítě budou připojena pouze autorizovaná zařízení. Autentizace infrastruktury veřejných klíčů (PKI) je jedním z nejběžnějších používaných řešení. PKI používá digitální certifikáty k prokázání totožnosti zařízení. (Miller, 2016)

Kryptografické algoritmy se rozdělují do dvou kategorií:

- Symetrické
- Asymetrické

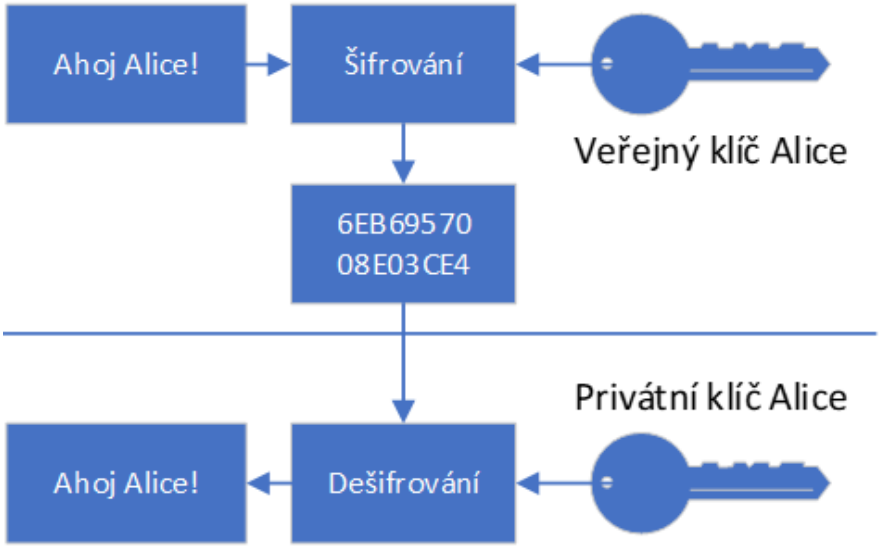
Symetrické algoritmy sdílejí jeden tajný klíč mezi komunikujícími klienty za účelem šifrování a dešifrování informací. Symetrické algoritmy jsou poměrně účinné z hlediska rychlosti a výpočetní síly, ale správa klíčů (bezpečná výměna a ukládání klíčů) je kritická. Pokud neoprávněná strana získá přístup ke klíči, komunikace již není chráněna. Symetrické kryptosystémy se obvykle používají k zajištění důvěrnosti.

Kryptografický klíč je tajná hodnota (v podstatě heslo) aplikovaná na kryptografický algoritmus. Síla a účinnost kryptografického algoritmu jsou do značné míry závislé na utajení a síle (nebo délce) klíče. Mezi příklady symetrických algoritmů patří Standard 3D šifrování dat, Advanced Encryption Standard (AES), Mezinárodní algoritmus šifrování dat (IDEA) a Rivest Cipher 5 (RC5). (Miller, 2016)

Asymetrické algoritmy používají kombinací veřejných a soukromých klíčů. Pouze veřejný klíč je třeba vyměňovat mezi komunikujícími vrstevníky a nemusí být uchováván v tajnosti (tudíž je to veřejný klíč). Komunikace jsou zašifrovány pomocí veřejného klíče, ale mohou být dešifrovány pouze soukromým klíčem. Asymetrické algoritmy jsou výpočetně intenzivnější než symetrické algoritmy, ale nemají stejné problémy se správou klíčů. Asymetrické kryptosystémy se typicky používají k poskytnutí autentizace. Některé asymetrické algoritmy, jako je RSA, vyžadují větší kryptografický klíč, který poskytuje stejnou úroveň bezpečnosti jako symetrické algoritmy. Zjednodušeně lze říci, že pro stejnou velikost klíče jsou asymetrické algoritmy obvykle méně spolehlivé než symetrické

algoritmy. Například 1024bitový asymetrický klíč může poskytnout zabezpečení ekvivalentní 80bitovému symetrickému klíči.

Výměna klíčů je protokol používaný ke sdílení tajného klíče mezi klientem a serverem bez přenosu klíče. Tento tajný klíč se pak používá v symetrických kryptosystémech pro účely důvěrnosti (šifrování komunikačního spojení mezi klientem a serverem).



Obrázek 13 - Princip asymetrického šifrování
Zdroj: https://upload.wikimedia.org/wikipedia/commons/thumb/5/52/Asymetrick%C3%A1_kryptografie.svg/330px-Asymetrick%C3%A1_kryptografie.svg.png

Kryptografická funkce hashování je jednosměrná operace používaná k digitálnímu podpisu a ověření integrity informací. Typické využití hashů zahrnuje digitální podpisy a ověření heslem (hash je kratší zastoupení dlouhého hesla, které poskytuje vyšší úroveň zabezpečení, protože nevyžaduje zveřejnění všech bitů v dlouhém hesle). Jestliže má být hash efektivní, musí mít několik vlastností:

- **lze ho snadno vypočítat** (jakákoli daná zpráva může být reprezentována hashem s pevnou délkou);
- **nevratný** (prakticky nemožné vygenerovat původní zprávu z hash);
- **nezměnitelný** (téměř nemožné změnit původní zprávu, aniž by došlo ke změně hash);
- **unikátní** (prakticky nemožné pro dvě různé zprávy generovat stejný hash). (Miller, 2016)

2.2 Standardizační normy

Standardizační normy jsou výsledkem procesu tzv. standardizace. Standardizační proces vzniká díky seskupení informací ve společnosti. Hlavním důvodem vzniku těchto norem je především usnadnění výroby, komunikace, obchodu a měření. Právě z těchto důvodů vyplývá několik výhod. Jsou to výhody především v utváření výrobních vzorců a předcházení problémů či jejich řešení. Nicméně hlavní nevýhodou, zejména pro výrobce, je jejich cena. Neboť instituce, které tyto normy utvářejí si také svou práci nechají zaplatit. Což pro společnost, vytvářející zařízení, znamená další investici.

Standardizační normy můžeme rozdělit do několika kategorií:

- **De iure** – standardy, tvořeny skupinou pověřených expertů různých organizací, věnující se standardizaci. Mezi De iure normy patří například ISBN.

- **De Facto** – standardy, určené praxí a rozšířením mezi veřejnost. Takovýmto standardem je například formát .mp3.

- **Proprietární standardy** – vlastněné výhradně organizací či jednotlivcem, jenž se věnuje standardizaci. Použití dané normy je podmíněno poplatkem či licencí.

- **Otevřené standardy** – veřejně přístupné s kompletní dokumentací. Příkladem je protokol IP, který hraje hlavní roli v oblasti internetu. (Cihi, 2017)

2.3 Společnosti popisující bezpečnost IoT a jeji části

Jestliže by se jednalo o popis bezpečnostních norem IoT, bohužel v praxi neexistuje žádná norma, popisující přímo tuto technologii. Jsou dva případy, kdy se společnosti snažily o jakousi „standardizaci“, nicméně ani jeden případ není formálně uznáván jako norma pro IoT. Prvním případem jsou standardy použité technologiemi, díky nimž je realizován IoT. Vhodným příkladem této technologie je například WiFi, podléhající standardu IEEE 802.11. Druhým případem je vytvoření tzv. pokynů pro bezpečnou práci, což je soubor

pravidel pro návrh a realizaci IoT. Svým rozsahem a komplexností se podobá bezpečnostní normě, nicméně formálně uznanou normalizační institucí není.

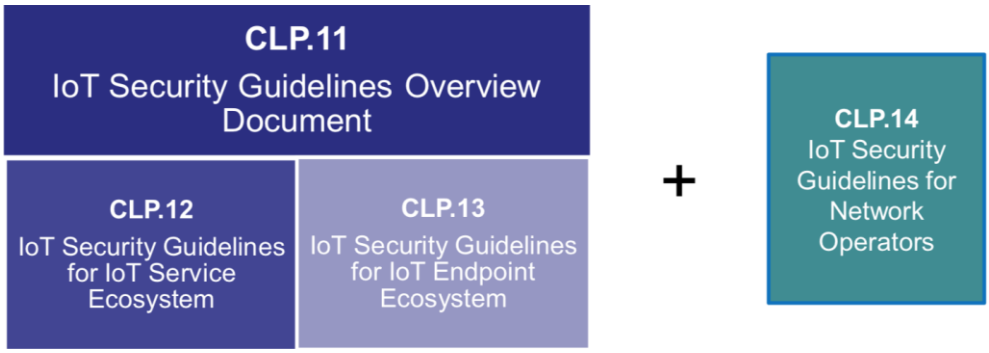
Společnost, která se o standardizaci IoT zajímá nejvíce, je asociace se zkratkou GSMA. Zkratka GSMA znamená „Global System for Mobile Communication“ a zabývá se mobilními komunikacemi. Nicméně v případě IoT je to právě ona druhá kategorie v pokusu o „standardizaci“, což je vydání bezpečnostních pokynů pro návrh a realizaci. Jejich postup je oficiálním dokumentem vydaným GSMA a je volně dostupný veřejnosti s názvem „IoT security guidelines“. Právě těmito pokyny začíná tato kapitola.

2.3.1 GSMA Security Guidelines

Dokument od společnosti GSMA se skládá ze 4 částí. První část dokumentu je určena k tomu, aby pomohla společnosti porozumět rodícímu se odvětví IoT a aby společně porozuměla otázkám bezpečnosti internetu. Sada dokumentů s pokyny podporuje metodiku rozvoje bezpečných služeb IoT, která zajistí, aby se osvědčené postupy v oblasti bezpečnosti staly součástí celého životního cyklu služby. Dokumenty poskytují doporučení, jak zmírnit společné bezpečnostní hrozby a slabiny v rámci služeb IoT. (Childs, 2017)

Struktura sady dokumentů GSMA pro bezpečnostní pokyny je uvedena na obrázku č.14. Doporučuje se, aby dokument CLP.11, což je úvod do bezpečnosti IoT, byl přečten jako první ještě před přečtením podpůrných dokumentů.

Cílem tohoto dokumentu je poskytnout výrobci technologie nebo služby IoT sadu návrhových pokynů pro vytváření bezpečného produktu. K plnění tohoto úkolu bude tento dokument sloužit jako zastřešující model pro interpretaci aspektů technologie nebo služby, které jsou pro realizátora relevantní. Jakmile jsou tyto aspekty nebo komponenty identifikovány, implementátor může vyhodnotit rizika spojená s každou složkou a je schopný určit, jak je kompenzovat. Každá komponenta může být rozdělena na dílčí součásti, kde budou popsána její další rizika. Každému riziku bude přiřazena priorita, která pomůže výrobci při určování nákladů útoku, stejně jako nákladů na nápravu.



Obrázek 14- Struktura dokumentů GSMA
Zdroj: https://www.gsma.com/iot/wp-content/uploads/2019/01/CLP.11-v2.0.pdf

Rozsah tohoto dokumentu je omezen na doporučení týkající se návrhu a implementace služeb IoT. Tento dokument není určen k tomu, aby vedl k vytváření nových specifikací nebo norem IoT, ale bude odkazovat na aktuální řešení, normy a osvědčené postupy. (Childs, 2017)

Nejprve je důležité upřesnit pro koho je dokument GSMA určen. Primárními čtenáři dokumentu od GSMA jsou:

- Poskytovatelé služeb IoT – podniky nebo organizace, které se snaží rozvíjet nové a inovativní propojené produkty a služby.
- Výrobci zařízení IoT – poskytovatelé zařízení IoT.
- Vývojáři IoT – ti, kteří vyvíjí služby IoT.
- Provozovatelé sítí, kteří jsou sami poskytovateli služeb IoT nebo vytvářejí služby IoT.

GSMA každé důležité části systému IoT věnuje vlastní pokyny. Části systému jsou popsány v první kapitolena obrázku č.4 schéma IoT. Tyto části jsou: systém služby, systém koncového bodu a síťový operátor.

Dnešní pojetí IoT vyžaduje jakýsi základní ekosystém, z kterého vyplývá význam, funkčnost a přidaná hodnota pro koncová zařízení, výrobce, a především pro uživatele. V závislosti na složitosti aplikací a služeb, může být jejich infrastruktura obrovská, a především složená z mnoha odlišných typů služeb a přístupových bodů. Bez ohledu na formát, službu a její základní ekosystém funguje jako zprostředkovatel funkčnosti a komunikace pro každou

základní oblast v IoT. Ostatní služby můžeme nazvat „podsystémy“ a závisí na jednom daném základním ekosystému, řídící kompletní hierarchii autentizace, připojení mezi uživateli, dostupnost a další úkoly pro každodenní provoz IoT. GSMA navrhla model případné infrastruktury a složky, které by měly obsahovat. Tyto složky však závisí na daném řešení a v práci uvádí tedy jen příklady:

- webová služba;
- aplikační server;
- databáze;
- autentizační server;
- síťový server;
- aplikace třetí strany (např. software k fakturaci).

K zajištění bezpečnosti by měly být tyto složky zvlášť izolovány samy od sebe. Jestliže se totiž jeden ze serveru stane obětí útoku, nezpůsobí to kolaps celého systému. GSMA také doporučuje obranu proti určitým typům útoků, na které by se měli správci infrastruktur soustředit. Mezi tyto doporučení patří: ochrana proti DDOS útokům, způsob vyrovnání zatížení serveru, redundance a možnosti firewallu.

Další částí je systém koncového bodu. Bezpečnostní výzva, jenž představuje IoT, je v mnoha případech přímo spojena se specifickými charakteristikami koncového bodu IoT, jenž služba používá. Například mnoho koncových bodů IoT má následující charakteristiky, které jim přinášejí zvláštní bezpečnostní problémy a výzvy:

Nízká energetická náročnost – Nízká spotřeba energie může být požadavkem k dosažení dlouhé životnosti baterie (několik let) u vzdáleného nepřístupného koncového bodu bez trvalého napájecího zdroje nebo proto, že má zařízení trvalé, ale omezené napájení (např. zásobování solární energií).

Nízké náklady – Některé obchodní nároky kladou důraz na nízké náklady na pořízení takového IoT zařízení. To často vede k tomu, že zařízení obsahuje nízkou kapacitu zpracování, malé množství paměti a omezený operační systém.

Dlouhá životnost – Mnoho koncových bodů pro průmyslové či městské využití musí mít dlouhou životnost. To představuje výzvu v podobě zajištění takového šifrování, které bude po celou dobu životnosti zařízení funkční. Další výzvou je správa takovýchto zařízení a jejich aktualizace.

Fyzický přístup – Jako poslední je samozřejmě situace, kde jsou zařízení fyzicky přístupné danému útočníkovi. Všechny hardwarové komponenty a rozhraní na těchto koncových bodech jsou proto potenciálně předmětem útoku a musí být zabezpečeny výrobcem.

Výsledek výše zmíněných bodů je, že v mnoha službách a zařízeních koncové body nejsou přímo připojeny ke komunikační síti a mnoho koncových bodů ani nemá možnosti protokolu IP (dosažitelnost v rámci síti). Z těchto bodů a z nesourodosti IoT vyplývá model, který kategorizuje IoT do tří skupin: komplexní koncové zařízení, výchozí brána a koncové zařízení s nízkou energetickou náročností.

Komplexní model koncového zařízení je zařízení typické potřebou nepřetržitého připojení k serveru back-end přes komunikační spojení na dlouhé vzdálenosti, jako jsou například mobilní data, Wi-Fi anebo Ethernet. Zařízení má v sobě obvykle procesor a je schopno provozovat komplexnější výpočty, jelikož je připojeno k napájecímu zdroji či obsahuje baterii s přístupem k pravidelnému nabíjení.

Příklady komplexních koncových bodů:

- IoT osvětlení;
- spotřebiče;
- průmyslové systémy;
- chytré auto.

Díky komplexnosti systémů je také v těchto systémech jednodušší implementace šifrování a celková bezpečnost zařízení.

Výchozí bránou se rozumí zařízení, které je typicky připojeno k dedikovanému zdroji napětí, jako most do internetu a spravuje zařízení uvnitř v síti. Funkce výchozí brány lze shrnout do několika bodů:

- vyhledávání zařízení;
- ovládání a nasazení do sítě;
- správa a monitoring zařízení;
- autentizace a zabezpečení.

Zatímco výchozí brány jsou technicky koncové body, nemusí být nutně řízeny koncovým uživatelem a mohou být spravovány poskytovatelem služeb IoT nebo provozovatelem sítě. Bez ohledu na to mohou být brány také navrženy jako komplexní koncové body, aby efektivněji využívaly distribuci sítě na více koncových bodech s nízkou energetickou náročností v lokální síti.

Stejně jako komplexní koncové body, výchozí brány jsou schopny většího zpracovatelského výkonu. To umožňuje výrobcům relativně snadno implementovat komplexní řešení zabezpečení.

Tyto vlastnosti výchozí brány také umožňují výrobcům zahrnout více komunikačních technologií pro směrování zpráv mezi různými typy síťových zařízení. To umožňuje komunikaci mezi koncovými body, které by normálně nemohly efektivně komunikovat. Tímto způsobem brány fungují jako agregační bod pro zařízení v rámci místního ekosystému, což jim umožňuje komunikaci mezi službou a sítí. V rámci výchozí brány existuje několik hrozeb.

První a nejjednodušší krok při pokusu o ohrožení koncového bodu IoT obvykle zahrnuje slabiny v komunikačním modelu. Útočník sleduje, zda komunikační model zahrnuje osvědčené postupy komunikace v oblasti bezpečnosti. Pokud může útočník snadno zachytit přihlašovací údaje, komunikační tokeny nebo jiné identifikátory, které služba používá k ověření koncového bodu, ohrožuje tím zařízení.

Dalším typem hrozby je konzolový přístup. Nicméně nejedná se přímo o útok nýbrž o strategii, pro niž je typické, že některé zařízení obsahují přístup do konzole. Je to z důvodu diagnostiky vývojářů a techniků zajišťujících kvalitu, schopnost diagnostikovat anomálie hardwaru nebo softwaru. Informace získané z konzole jsou pro útočníka velmi cenné. Kromě toho může konzola poskytnout protivníkovi možnost přihlásit se do systému lokálně i vzdáleně.

V mnoha případech se jedná o jednoduchý přístup k portu konzole a potenciální útočník má přímý přístup k příkazovému řádku na zařízení. V jiných případech jsou vyžadovány přihlašovací údaje, nicméně v praxi jsou tyto údaje snadno uhodnutelné. Pokud jiný uživatel na internetu zjistí přihlašovací údaje, tak v praxi bývají všechny přihlašovací údaje koncových zařízení stejné. Jediné, co musí potenciální útočník udělat je, že použije vyhledávač Google a zjistí, zda někdo jiný tyto data nezveřejnil.

Pokud se nelze dostat do příkazové řádky pomocí konzole probíhá nejčastěji analýza ostatních I/O portů. Pomocí I/O portů se lze přímo připojit do obvodu zařízení, a tak ho také nějakým způsobem ohrozit. Nejjednodušší útok je zjištění, zda je přítomno zapisovatelné médium. Například karta s externí pamětí (SD / MMC), na kterou lze zapisovat. Nebo to můžou být čipy NVRAM nebo EEPROM a jejich konfigurace, umožňující přístup k příkazovým řádkům nebo přístup k bezpečnostním klíčům.

Poslední kategorií jsou zařízení s nízkou energetickou náročností. Typem tohoto zařízení je senzor nebo jednoduché fyzické zařízení (např. například spínač světel). Spínač světel je velice elementární a nedisponuje velkým množstvím funkcí. Účelem těchto zařízení je sloučit jedinečný fyzický účel a poskytnout data službě pro následné vyhodnocení spotřebitelem či zaslání dat výchozí bráně. V těchto typech zařízení jsou obvykle použity levné procesní jednotky a konektivity zajištěny pomocí osobní sítě PAN či Bluetooth apod. nízkoenergetické technologie. Zabezpečení těchto typů zařízení je těžkým úkolem pro výrobce, neboť nízkoenergetická náročnost omezuje implementaci složitějších ochranných řešení. V praxi to pak je pouze zabezpečení za použití hesla. Nicméně tato zařízení díky své nenáročnosti a použití pouze na „jednu“ činnost nepředstavují velkou hrozbu.

Hlavním prvkem v mobilní síti je tzv. „International Mobile Equipment Identity“, volně přeloženo jako mezinárodní mobilní identita. IMEI bylo původně zavedeno jako jedinečná identita terminálu, připojená do sítě GSM. Operátoři tak dokázali rozlišit neschválené zařízení. V současné době se IMEI používá k identifikaci mobilních zařízení. Zařízení, která jsou získáná neoprávněně je možné vzdáleně „zablokovat“ právě pomocí zmíněného IMEI čísla. To umožňuje i operátorům schopnost vzdáleně ovlivňovat připojení IoT zařízení, což může být potenciální hrozba.

V případě mobilního operátora se jedná o základní bezpečnostní prvky, nad kterými by se operátor měl zamýšlet. Základní bezpečnostní mechanismy v síti jsou:

- Identifikace a autentizace subjektů zapojených do služby IoT (tj. výchozí brány, koncová zařízení, domácí síť, roamingové sítě, servisní platformy).
- Řízení přístupu k různým entitám, které je potřeba připojit k vytvoření služby IoT.
- Ochrana dat s cílem zaručit bezpečnost (důvěrnost, integritu, dostupnost, pravost) a soukromí informací v rámci sítě IoT.
- Procesy a mechanismy, které zaručují dostupnost síťových zdrojů a chrání je před útoky (například nasazením vhodné brány firewall, technologie prevence vniknutí a filtrování dat)

Identifikace se skládá z poskytování jedinečných identifikátorů subjektům v rámci služby IoT a korelace těchto elektronických identit s reálnými. V mobilní připojené službě IoT jsou koncová zařízení většinou identifikována pomocí IMEI. Sítě jsou identifikovány pomocí síťových kódů a kódů zemí.

Identita hraje rozhodující roli v procesu autentizace, neboť bezpečná autentizace může být dosažena pouze na základě bezpečné identity. Je proto nezbytné, aby identity (například IMEI) vydané a používané v rámci služby IoT byly bezpečně chráněny před neoprávněnou úpravou, předstíráním identity nebo krádeží.

Praktický problém, se kterým může poskytovatel služeb IoT setkat je, že jejich služba IoT může vyžadovat komunikaci s mnoha servisními platformami, z nichž každý může vyžadovat samostatnou jedinečnou identifikaci. Všechny identity používané pro vytvoření komunikačního spojení pro každou platformu služeb IoT pak bude muset být bezpečně zajištěna, uložena a spravována službou IoT. Řešením pro tento problém jsou tzv. „Single sign-on“ služby. Jsou to služby poskytovány provozovateli sítí umožňující koncovým zařízením prokázat svoji totožnost jednou. Následná připojení by probíhala bez nutnosti prokázání své identity.

Síťoví operátoři poskytují komunikační bezpečnostní mechanismy pro mobilní sítě, které zajišťují kombinaci integrity, důvěrnosti a autenticity. Kde je to vhodné, provozovatelé sítí

poskytují a spravují zabezpečené připojení k podnikovým sítím pomocí virtuálních privátních sítí (VPN) a šifrovaných internetových připojení.

Účelem zabezpečeného komunikačního kanálu je zajistit, aby data odesílaná přes kanál nebyla zpracována, používána nebo přenášena bez vědomí a souhlasu subjektu údajů. Technologie šifrování hraje zásadní roli při zabezpečeném přenosu dat a zajišťuje tak vlastnosti důvěrnosti, integrity a autenticity. Šifrování musí odpovídat navrhovanému a nasazenému systému s přihlédnutím ke koncovému bodu, síťovým aspektům a poskytované službě.

Provozovatelé sítí mohou výrobcům služeb IoT poskytovat služby šifrování dat, aby zajistili integritu komunikace a odolnost sítě.

Provozovatelé sítí tradičně poskytují veřejnou telekomunikační infrastrukturu nebo směs infrastruktury veřejných nebo soukromých sítí. Mnoho provozovatelů sítí může zajistit, aby data zákazníka/uživatele, která prochází infrastrukturou veřejné sítě, byla šifrována mezi okamžikem, kdy data vstupují do infrastruktury veřejné sítě až do okamžiku, kdy opouští síť. V případě potřeby mohou provozovatelé sítí rovněž nabízet pomoc poskytovatelům služeb IoT nasazením nebo odvozením vlastních šifrování, aby se zajistila důvěrnost údajů IoT při tranzitu prostřednictvím infrastruktury provozovatele sítě.

Provozovatelé sítí mohou svým zákazníkům poskytovat soukromé sítě, ve kterých jsou k dispozici vyhrazené komunikační kanály pro použití jednoho zákazníka. Dochází tak k zajištění, že žádná data nebudou procházet veřejnou sítí, jako je internet. Existuje několik typů soukromých sítí:

1. Vytvoření tzv. tunelu za použití protokolu L2TP (Layer Two Tunneling Protocol) a zabezpečení tohoto způsobu za použití protokolu IPsec (Internet Protocol Security), což je internetový protokol, který slouží k zabezpečení sítí.
2. Poskytování tzv. E2E bezpečnosti mezi zákazníkem a aplikačním serverem
3. Vytvořením vyhrazené sítě pro službu IoT nasazením samostatné instance sítě se sdílenou rádiovou sítí.

Bezpečnostní doporučení mobilní sítě je závěr kapitoly o bezpečnostních postupech firmy GSMA. Problematika bezpečnostních mechanismů v dokumentech GSMA je velmi obsáhlým tématem a popis každého bezpečnostního mechanismu by pro čtenáře neznamenal další přidanou hodnotu. Výše uvedené odstavce jsou především krátkým shrnutím problematiky bezpečnosti IoT a slouží jako náznak její standardizace. V případě detailnější analýzy, praktických příkladů zabezpečení a jejich použití v praxi je nutné nastudování přímo zmíněných dokumentů. Nicméně dokumenty výborně slouží jako úvod do problematiky bezpečnosti IoT a dokáží čtenářovi vytvořit „nadhled“ nad touto problematikou. (Childs, 2017)

2.3.2 Použité technologie a jejich normy

V předešlé kapitole byly popsány doporučené postupy pro vytváření a provozování IoT, nicméně nejednalo se o postupy, které by byly oficiálně standardizovány. Tato kapitola se věnuje problematice technologií, použitých v IoT a jejich bezpečné použití je standardizováno. K popisu technologií a jejich standardů použijeme 5 vrstvou architekturu IoT. 5 vrstvá architektura byla popsána na obrázku č.3 a v nadcházející tabulce jsou vyjmenovány vrstvy s jejich krátkým popisem, použitou technologií a standardy použité danou technologií. Dále je uveden popis každého standardu zvlášť.

Tabulka 1 - Architektura IoT, její technologie a standardy

Jméno vrstvy	Funkce	Technologie	Standard
1. Fyzická	Identifikace objektů, získání dat ze senzorů	RFID Tagy, Senzory	ISO 14443 a ISO 15693
2. Transportní /Síťová	Přenos dat ze senzorů do vyšší vrstvy	3G, 4G LTE, Wi-Fi, Bluetooth, ZigBee atd.	DTLS, IPsec, RPL Security
3. Procesní	Management služby a ukládání dat	Databáze	-
4. Aplikační	Reprezentace dat	Platformy	-
5. Obchodní	Analýza a zpracování dat výrobcem	Obchodní modely, grafy atp.	-

Zdroj: Vlastní

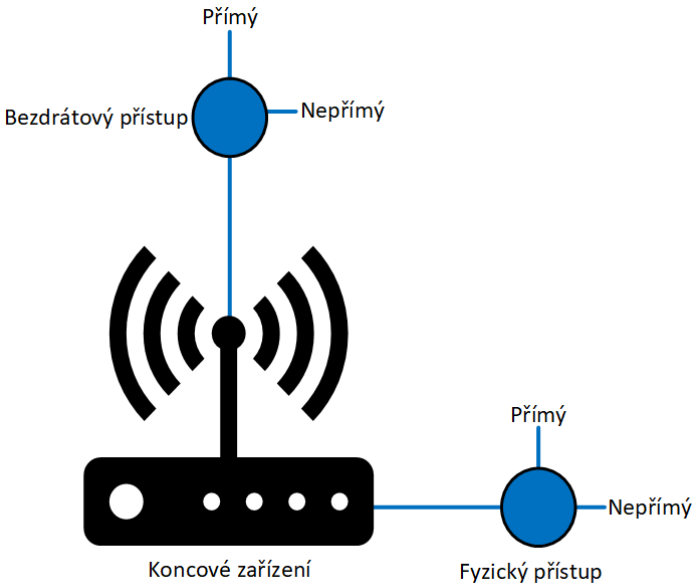
Pro účely této diplomové práce je výsledná tabulka dostačující a uzavírá tak kapitolu o standardizaci IoT. Detailnější popis každé normy je pro tuto práci bezpředmětný, neboť se jedná o rozsahově velmi obsáhlé dokumenty a většinou jde o myšlenkově stejné záležitosti, které jsou popsány v předešlé kapitole.

3 Analýza rizik Internetu věcí

Následující kapitola, s názvem Analýza rizik Internetu věcí, se zabývá kompletním řešením IoT, přičemž vychází z diagramu IoT řešení. V předešlé kapitole se jednalo o obsáhlé seznámení s bezpečností IoT a se snahami veřejnosti o standardizaci tohoto trendu. Tato kapitola spojuje předešlé dvě kapitoly v jednu a poskytne tak detailnější analýzu zaměřenou na technickou stránku věci, nastínění možných rizik, které plynou z IoT, a také vyjmenování typů útoků. Celkově je tato kapitola rozdělena do 3 skupin, přičemž první 2 skupiny se týkají analýzy každého článku IoT a poslední skupinou bude analýza celkového řešení dohromady.

3.1 Analýza technických prostředků koncového zařízení

První kapitola se zabývá technickými prostředky koncového zařízení v IoT. K tomu dopomůže high-level zobrazení na obrázku č.15.



Obrázek 15 - Schéma koncového zařízení
Zdroj: Vlastní

V tomto schématu lze dělit koncové zařízení na dvě skupiny, a to dle způsobu přístupu. Zaprvé je to přístup bezdrátový a zadruhé přístup fyzický. Tyto skupiny se budou dále dělit na přímé a nepřímé. Tento typ dělení vychází z postoje útočníka vůči samotnému zařízení. Jak bylo zmíněno, první skupinou je přístup bezdrátový. Přímý bezdrátový přístup

je přístup, kdy má útočník plný přístup k bezdrátové sítí vytvořené koncovým zařízením. Útoky tak realizuje za pomocí technologií, vytvářející tyto sítě. Tyto technologie jsou například Wi-Fi, Bluetooth apod.

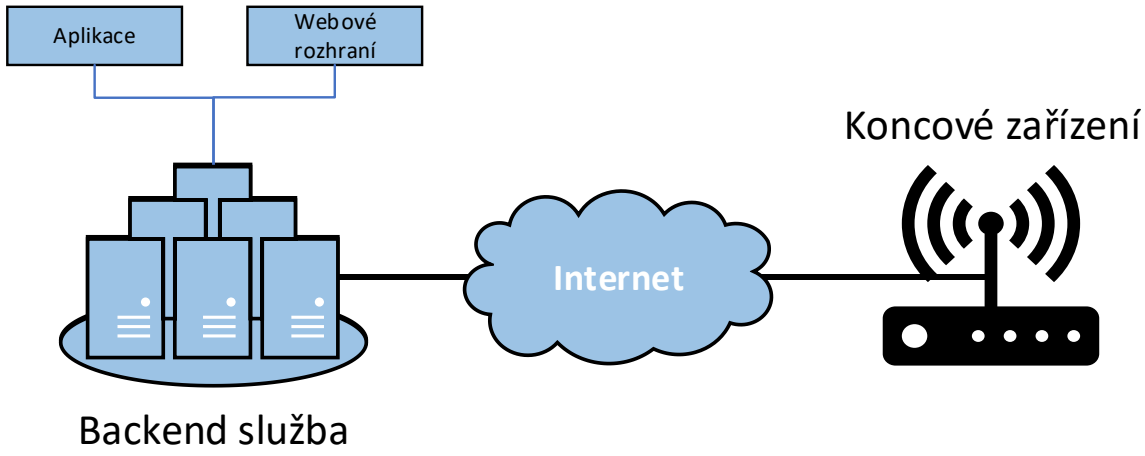
Při nepřímém bezdrátovém přístupu je způsob útoku realizován skrze využití prostředníka, resp. dalšího zařízení IoT. Jestli je další zařízení připojeno drátově či bezdrátově, to pro útočníka není důležité. Pro útočníka je důležité, zda toto zařízení je připojeno k předmětu jeho úmyslu, tedy koncovému zařízení.

Další skupinou je přístup fyzický, taktéž rozdělený na přímý a nepřímý. V případě přímého fyzického přístupu se jedná o situaci, kdy útočník je přímo u koncového zařízení a toto zařízení obsahuje možnosti k útoku. Mezi tyto možnosti mohou patřit například port Ethernet, čtečka SD karet či USB port. Pokud zařízení nemá tyto porty nijak zvlášť chráněné, útočník je tak schopný velmi jednoduchým způsobem toto zařízení ovládnout. Tedy za předpokladu, že má útočník k tomuto zařízení fyzický přístup. S nepřímým fyzickým přístupem je to tedy analogicky jako u případu nepřímého bezdrátového přístupu, kdy útočník se fyzicky dostane k jednomu ze zařízení, které je ve společné síti se zařízením koncovým a za využití tohoto faktu se k němu může dostat.

3.2 Analýza technických prostředků poskytovatele služeb

Další řetězec IoT je zprostředkovatel služeb. V této analýze vystupují tři objekty. Prvním objektem je, v minulé kapitole popsané, **koncové zařízení**. Dalším objektem je **internet** a jako poslední předmět této kapitoly, zprostředkovatel služeb, který je v následujících nazývám jako tzv. **backend služba**. Obrázek č.16 představuje komunikaci mezi zprostředkovatelem služeb, což může být výrobce zařízení anebo také externí firma, přicházející s platformou IoT, a mezi koncovým zařízením. U backend služby je také vyobrazený způsob přístupu k datům. Je to možnost za použití aplikace, kterou zařízení podporuje, či možnosti webového rozhraní. Tyto způsoby jsou závislé na rozhodnutí výrobce. Mezi koncovým zařízením a backend službou probíhá obousměrná komunikace, kdy zařízení posílá získaná data ze senzorů prostřednictvím internetu zpět. Backend služba následně data vyhodnocuje a zasílá je upravená zpět směrem ke koncovému zařízení. Příkladem mohou být například senzory z chytrého auta. Příkladem

jsou senzory zabudované do chytrého auta, v němž je nastavená funkcionalita limit rychlosti. Tato funckionalita je schopna rozpoznat, zda řidič překročil předem nastavenou rychlost. Vyhodnotí tedy porušení limitu a spolu s časovou stopou zašle, prostřednictvím internetu, informaci backendslužbě. Backendslužba poté vyhodnotí uživatele a kontaktuje ho. Kontaktování uživatele nastane pouze v rámci aplikace, nicméně ve webovém rozhraní se tato informace uloží a je uživateli dostupná.



Obrázek 16 - Schéma zprostředkovatele služeb
Zdroj: Vlastní

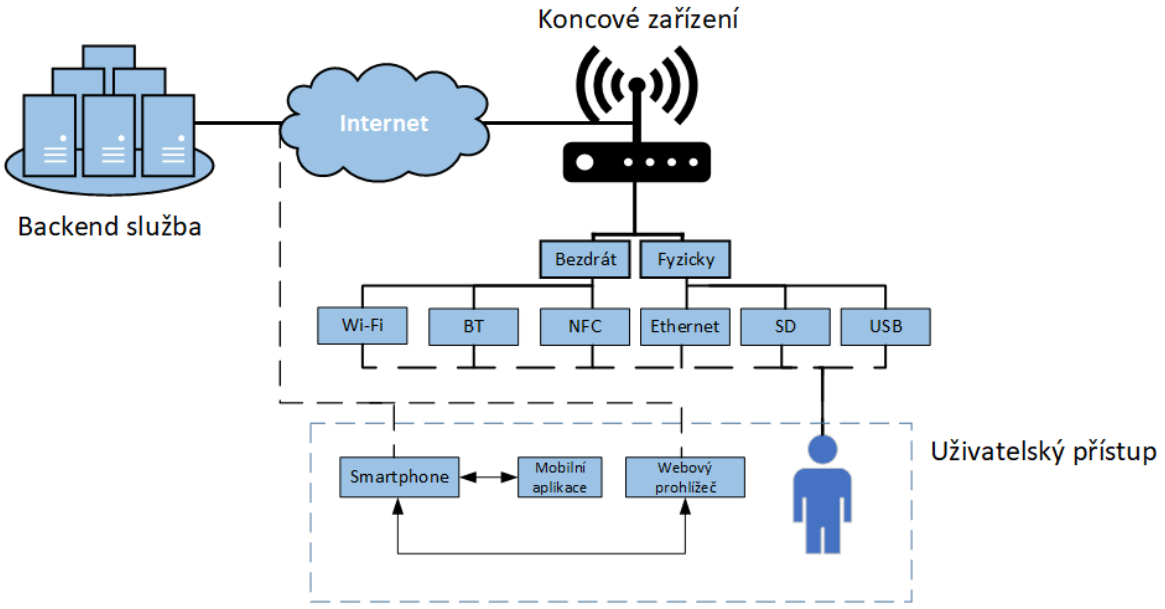
3.3 Celkové řešení IoT

K definici rizik je potřeba rozvinout předešlé schéma tak, aby v něm byly zakomponovány další objekty včetně uživatele. Uživatel v obrázku č.17 vystupuje v podobě uživatelského přístupu a má několik možností, jak ovlivnit koncové zařízení a taktéž má přístup k backendové službě.

Prvním způsobem je smartphone. Jak bylo uvedeno v první kapitole, v dnešní době je trend především v ovládání IoT zařízení a celého jeho systému pomocí smartphonu. Tato funkcionalita a její řešení závisí na typu zařízení. Jsou totiž dvě možnosti, jak smartphone dokáže ovlivnit koncové zařízení. První možností je vzdálený přístup pomocí mobilních dat, při které se uživatel připojuje k backend službě. Druhou možností je, že je dané koncové zařízení řešeno jako součást v domácí síti. To znamená, že k němu není možné přistupovat

pomocí internetu, ale jen v rámci dané domácí sítě, ke které jsou obě zařízení připojena. Tento princip je řešen jak pomocí mobilní aplikace, tak pomocí webového prohlížeče. Každopádně v případě webového prohlížeče se může jednat i o jiné zařízení, než je smartphone.

Další odlišnost mezi schématy je v samotném koncovém zařízení. Na předešlém obrázku se zkoumá pouze koncové zařízení. Na obrázku č.17 je zobrazeno koncové zařízení a jsou rozepsané jeho možnosti připojení, popsáné v předešlé kapitole. Tyto možnosti jsou zaprvé bezdrátové připojení a zadruhé připojení fyzické. V rámci schématu jsou zde do další úrovně rozepsané pouze některé technologie, jako je Wi-Fi, BT, NFC. Nicméně patří zde i technologie uvedené v předcházející kapitole o technologiích v IoT. To samé platí pro fyzické připojení. Je důležité si uvědomit, že nezáleží na typu technologie, díky které se koncovému zařízení přistupuje, ale vše závisí na typu ochrany přístupu k technologii, protože ve výsledku jsme vždy připojeni k danému zařízení. To je i důvod, proč se následně technologie setkávají a propojují do jedné a končí u uživatele. Tento fakt totiž znamená jedno – vždy je to jen v první řadě o výrobci a o uživateli. Na jedné straně o uživateli provozující zařízení a na straně druhé uživatel jako výrobce, který zařízení vyrábí a zabezpečuje.



Obrázek 17 - Schéma kompletního řešení Internet of Things
Zdroj: Vlastní

3.4 Definice rizik a způsobů útoku

Předešlá kapitola byla o analýze řešení IoT, způsobu komunikace a jeho high-level zobrazení. Jelikož je analýza hotová a s určitým nadhledem se dá použít jako univerzální řešení pro všechna IoT. Nyní je prostor pro definování rizik způsobena tímto řešením. Rizika lze kategorizovat podle roviny, kde je útok uskutečňován:

- **Fyzické objekty** – tato kategorie se zaměří na identifikaci všech fyzických útoků směřovaných na hardware. RFID tagy, čtečky RFID, mikro kontroléry, akční členy a senzorové uzly patří mezi příklady takových objektů.
- **Protokoly** – tato kategorie je věnována všem možných útoků na protokoly IoT. Tyto protokoly slouží k připojení, vytváření sítí a směrování. Také protokoly, sloužící aplikační a transportní vrstvě, které jsou v navrhované architektuře. Dále protokoly známé jako komunikační, a v neposlední řadš protokoly webových služeb.
- **Data –** tato kategorie definuje útoky směřované na data. Z předešlých kapitol je známo, že jsou to data buď v backend službě či data v samotném zařízení.
- **Software** – tato kategorie se zaměřuje na identifikaci všech možných útoků na software IoT, včetně aplikací IoT umístěných buď v zařízeních IoT nebo také v backend službě, dále firmware, operační systémy, aplikační brány a služby.

V nadcházející kapitole jsou detailněji popsány útoky v každé kategorii. Tyto útoky jsou definovány na základě daného schématu ve spolupráci s předešlou kapitolou, ve které byly představeny některé principy bezpečnosti v IoT.

3.4.1 Fyzické objekty

V této kategorii jsou útoky primárně cíleny na hardwarové komponenty IoT systému.

Replikace objektu – v tomto typu útoku má útočník schopnost přidat do sítě nový objekt, který se identifikuje stejným způsobem jako objekt v síti IoT, jenž je autorizován. Toto zařízení by poté mohlo být zdrojem úniku citlivých informací.

Rušení RFID komunikace – posílání velkého množství dat přes rádiovou frekvenci používající RFID jako způsob komunikace. Toto zahlcení frekvence je hlavním cílem útoku.

Hardwarový trojský kůň – mnoho výzkumů ukázalo, že největší bezpečnostní problém v integrovaných obvodech je nízká odolnost vůči hardwarovému trojském koni. Hlavní cílem tohoto útoku je nepatrná změna v obvodu a následné získání přístupu k citlivým datům a firmwaru. Tento typ útoku se vyskytuje většinou jako tzv. zadní vrátka už při návrhu daného zařízení a tyto zadní vrátka pouze čekají na spuštění od jeho vývojáře.

Útok pomocí vyřazení jednoho z objektů IoT – tento útok má za cíl znefunkčnění sítě IoT. Útočník si vybere síť IoT a v této síti si najde objekt, sloužící jako most pro ostatní objekty. Vyřazením důležitého článku v síti způsobý nefunkčnost její velké části.

Útok za pomocí skrytého objektu – útok, realizován za užití fyzického objektu, který je zapojen do sítě a je skryt mezi ostatními objekty. Je tak použit jako klasický objekt sítě IoT a slouží útočníkovi jako odposlouchávací zařízení.

Neoprávněná manipulace s objekty – možnost, že útočník získá fyzický přístup k zařízení je v některých prostředí velká. Je to například v prostředí průmyslu, kde je rozmístěno více jak stovky objektů a senzorů a fyzický přístup k nim nepředstavuje žádnou překážkou. Takové objekty jsou snadným cílem. Nejznámější útoky jsou: změna firmwaru, změna operačního systému či stahování kryptografických klíčů.

Útok na vedlejší kanál komunikace – v IoT jsou z bezpečnostních důvodů integrovány některé bezpečnostní mechanismy. Je to například mechanismus, kdy kanál, na kterém probíhá výměna citlivých informací se liší od kanálu k výměně dat o identifikaci objektu. Útočník se tedy při útoku na objekt zaměří na tento „vedlejší kanál“.

Změna škodlivého kódu – útočník, v tomto typu útoku, mění kód daného objektu a získává tím jeho plnou kontrolu.

Klonování tagů – Dotýká se technologie NFC a RFID. Klonováním tagů, autorizováné systémem IoT, může vzniknout průnik do tohoto systému. Příkladem jsou chytré dveře, které

se otevírají za přiložení autorizovaného NFC tagu. Útočníkovi tak stačí pouze naklonovat tag z originálního zdroje a je oprávněn tyto dveře otevřít.

3.4.2 Protokoly

Na rozdíl od klasického internetu, který je navržen na neomezené množství objektů v síti, má systém IoT návrh architektury značně rozdílný. Tento návrh je možné vidět v tabulce č.2 Architektura IoT. V dané tabulce můžeme vidět několik protokolů rozlišených podle vrstev IoT. Tyto protokoly budou v této kapitole rozděleny do tří skupin. Protokoly připojení, komunikační protokoly a síťové protokoly.

Protokoly připojení se dají rozdělit do dalších dvou podkategorií: drátové a bezdrátové. Drátové připojení vyžaduje fyzické médium mezi objekty IoT, zatímco bezdrátové připojení je realizováno pomocí rádiových vln. Obě tyto technologie mají několik vlastností jako např. dosah, rychlost přenosu dat, spotřeba energie, podpora protokolu TCP/IP a také jsou rozdílné v topologiích.

Bezdrátové protokoly dále dělíme podle dosahu: NFC, RFID, Bluetooth, ZigBee a Wi-Fi.

NFC bylo navrženo tak, aby spolu dvě stejné technologie zabezpečeně komunikovaly. Nicméně technologie NFC trpí několika nedostatky, které jsou zmíněny na příkladech útoků.

Odposlouchávání – v systému NFC probíhá výměna dat mezi dvěma objekty v těsné blízkosti. Takový systém je náchylný k odposlechu. Komunikační kanál mezi dvěma objekty IoT vybavenými funkcí protokolem NFC je vůči tomuto útoku zranitelný, protože NFC chybí jakákoliv technika ochrany. Útočník může zachytit komunikační kanál pomocí silné antény nebo být v blízkosti komunikačního rozsahu.

Útok pomocí „prostředníka“ – přestože protokol NFC vyžaduje blízkost mezi dvěma komunikujícíma objekty, jsou tyto objekty teoreticky zranitelná vůči člověku uprostřed útoků. Útočník může zachytit data, upravit je a předat dalšímu objektu. Kromě těsné blízkosti, jenž je pro vykonání tohoto typu útoku nezbytná a vytváří tak útok velmi

obtížným, jsou zde také šifrovací techniky, které z už tak obtížného útoku dělají útok takřka neproveditelný.

Infikování dat – jestliže má útočník přístup ke komunikaci, má také schopnost tuto komunikaci rušit. Komunikační kanál mezi dvěma objekty se stává, díky změně přenášených dat, nečitelným.

Úprava dat – na rozdíl od infikování dat, v nichž útočník změní pouze formát přenášených dat. Modifikace těchto dat může změnit obsah.

Vkládání dat – během procesu výměny dat přenášenými mezi dvěma objekty vybavenými protokolem NFC. Útočník může do tohoto přenosu vložit některé údaje. Nicméně pouze v případě, že objekt vyžaduje dlouhou dobu k odpovědi. K úspěšnému vkládání dat může dojít tehdy, začne-li druhý objekt „odpovídat“. Pokud by totiž začala komunikace a útočník by vložil data a zasáhl tak originální zprávu, oba proudy by se překrývaly a data by se poškodila.

Protokol bluetooth je technologií na delší vzdálenost, díky tomu také vyžaduje autorizaci a stává se bezpečnější volbou. Nicméně žádný systém není dokonale bezpečný. Typy útoků jsou popsány níže.

Tzv. Bluesnarfing – hlavním cílem tohoto útoku je získat přístup nelegálně k zařízení Bluetooth tak, aby útočník mohl číst příchozí informace a přesměrovávat je na jiné zařízení.

Tzv. BlueBugging – představuje typ útoku využívající starší typy zařízení, kde jsou známé jejich zranitelnosti a dokáží se díky nim dostat do zařízení. Cíl útoku je sledovat telefonní hovory, posílat a přijímat zprávy a připojit se k internetu bez povědomí uživatelů.

Tzv. Bluejacking – v minulosti mnoho zařízení bluetooth byla navrhnuta k odeslání bezdrátové vizitky. Tento útok byl navržen tak, aby zasílal škodlivé vizitky. Nicméně takový útok nedával útočníkovi citlivé informace. Jelikož se jedná o typ útoku na starší verze Bluetooth je zde omezení, které vyplývá ze starších verzí. Tímto omezením je vzdálenost. Útočník musí být ve vzdálenosti maximálně 10 metrů od oběti. Jednoduchým řešením proti

tomuto útoku poté byla funckionalita nezjistitelnosti bluetooth zařízení, kdy se zařízení „skryje“ před ostatními, jedná se o tzv. nedetekovatelný režim. (Gupta, 2017)

Zasílání požadavků na autorizaci – v případě opakovaného odeslání žádosti o párování na zařízení oběti se může jednat o tzv. DOS útok. Jelikož oběť musí neustále požadavky odmítat, jednak to oběť připravuje o čas, ale také o kapacitu baterie v zařízení.

Odposlouchávání – nezašifrovaný přenos může být zachycen pasivním zařízením na odposlech.

Tzv. Spoofing – jednou z nejrozšířenějších zranitelností v technologii bluetooth s nízkou energetickou náročností je spoofing. Důvodem je, že tato zařízení vysílají signál veřejně.

Další technologií v pořadí je tzv. ZigBee, vytvářící PAN sítě. Jedná se o způsob propojení řádově větší než u technologie Bluetooth.

Zachytávací útok – vzhledem k tomu, že většina sítí ZigBee nepoužívá šifrovací algoritmy, mohou být zranitelné vůči těmto druhům útoků. Útočník může zachytit některé pakety k provádění škodlivých aktivit za pomocí vhodného softwaru.

Znovu vysílání paketů – je typ útoku, který závisí silně na zachycení síťového provozu. Když je možné paket zachytit, může útočník znovu vysílat zachycená data, jako by je odeslal autorizovaný uživatel.

Přesměrování komunikace – v síti ZigBee může útočník přesměrovat a odposlouchávat své pakety. Hlavním cílem tohoto útoku je zachycení a změna přenášených dat.

Útok na koncové ZigBee zařízení – hlavním cílem takového útoku je narušování a neustálé „kontaktování“ ZigBee koncového zařízení tím, že útočník pravidelně vysílá specifický signál, který zajistí přepnutí koncového zařízení z módu spánku na mód autorizace. Mód spánku slouží k šetření baterie, když už zařízení proběhlo autorizací.

V nadcházejících bodech jsou vysvětleny útoky založené na technologii Wi-Fi a jejího standardu 802.11.

FMS útok – zkratka složena ze jmen Fluher, Mantin a Shamir. Ten představuje typ útoku, jenž je založen na kryptografickém protokolu WEP. Využívá přitom jeho slabin, kdy je útočník schopen zjistit kryptovací klíč a rozklíčovat tak heslo a tím se dostat do sítě.

Útok Korek – Zmíněným korkem je chápán neznámý účastník bezpečnostního fóra NetStumbler.org, jenž objevil útok na Wi-Fi sítě s kryptovacím protokolem WEP. Je to útok velmi podobný metodě FMS, ale rychlejší.

Fragmentační útok – jedná se o typ útoku, který pojednává v kontextu s protokolem WEP. V první řadě je třeba odposlouchávat komunikaci a zachytávat pakety. Všechny pakety přenášené přes sítě 802.11 mají totiž homogenní záhlaví a pomáhají útočníkovi odhadnout prvních 8 bajtů záhlaví. (Gupta, 2017)

Slovníkový útok – použití techniky, díky níž může útočník může získat přístup do WiFi chráněné heslem tím, že hádá jeho přístupovou frázi. Jedná se o prosté tipování za použití vhodného slovníku, přičemž se software pokouší aplikovat miliony až miliardy různých kombinací

V předešlých odstavcích byly popsány bezdrátové technologie a protokoly, které souvisí s konektivitou a způsobem, jak daná zařízení komunikují. V následujících odstavcích jsou popsány protokoly síťové. Síťové protokoly popisují, jak jsou zařízení spojena jako celek a jakým způsobem komunikují. V tomto případě jsou řešeny dva typy síťových protokolů: tzv. **RPL** (Routing Protocol for Low power and lossy network) protokoly a tzv. **6loWPAN** (IPv6 over Low-power Wireless Personal Area Network). Oba výše zmíněné protokoly se zaměřují především na ty typy zařízení, která nejsou energiticky náročná. Nicméně druhý typ sítě představuje protokol nabízejíc více možností.

V případě RPL protokolu, se jedná o útoky:

Útok tzv. červí díry – RPL je náchylný k útoku, který narušuje topologii sítě i provoz. Tento útok lze spustit vytvořením soukromého kanálu mezi dvěma útočníky v síti a přesunutím selektivních paketů přes něj.

Útok identity – typ útoku, díky němuž může útočník získat přístup k paketům oběti. Cílem je útok na konkrétní zařízení s identitou, jež je převzata od oběti.

Zahlcení – využívá funkci kontaktování všech zařízení v síti. Kontaktované zařízení poté útočníka zařadí jako autorizované zařízení, přes které vysílá komunikaci a útočník ji tak může odposlouchávat.

Druhou kategorií je 6loWPAN protokol, který využívá protokol IPv6. Nicméně nejslabší stránkou tohoto protokolu je fakt, že neobsahuje funkcionalitu autorizovaného přístupu. V síti poté tato absence znamená dva útoky:

Autentifikační útok – vzhledem k chybějící autentizaci v 6loWPAN se všechny objekty mohou připojit k síti a získat oprávněný přístup.

Útok důvěrnosti – kvůli absenci šifrování technika v 6loWPAN, může být zahájeno mnoho útoků jako např. odposlouchávání či spoofing.

Poslední kategorií v části o protokolech jsou protokoly komunikační. Samotné protokoly jsou následně rozděleny na protokoly odlišující se v použitých vrstvách: od protokolů transportní vrstvy, až po protokoly vrstvy aplikační.

Transportní vrstva a její funkčnost je popsána v první kapitole této práce. Tato vrstva je zaměřena na problematiku protokolů TCP a UPD, jež jsou základním kamenem síťově komunikace nejen v IoT.

TCP – UDP Skenování portů – jedna z populárních metod, jenž prozkoumává porty komunikace. Za každým portem totiž stojí určitá služba v síti a za použití softwaru, který tento porty rozlišuje, může útočník kontaktovat daný port a zkoumat jeho možné slabiny.

UDP přetížení – způsob útoku, zahlcující UDP linku a její veškeré porty a znemožňuje tak dostupnost jiným službám/uživatelům.

Jak bylo zmíněno v první kapitole, aplikační vrstva hraje v IoT hlavní roli. Nejrozšířenější protokoly jsou MQTT a CoAP, které byly také vysvětleny.

Útok pomocí sdíleného klíče – bezpečnostní mechanismy na úrovni aplikační vrstvy jsou v některých případech řešeny pomocí sdílených klíčů. Tyto klíče jsou pak používány k různým autorizačním procesům. Klíče jsou v některých případech uloženy ve zdrojových kódech daného zařízení, což může být využito útočníkem k získání daného klíče.

Odposlouchávání – monitorování komunikace není výjimkou ani v těchto protokolech. Pokud se jedná o protokol CoAP, ten může funguovat i v tzn. Režimu no-security, kdy se zapne režim nevyžadující bezpečnostní mechanismy. Tato situace vede k tomu, že komunikace může být sledována, a to povede k odcizení osobních dat. V případě protokolu MQTT je zneužití velmi pravděpodobné. Jedná se o protokol, který je navržen absolutně bez jakýchkoliv bezpečnostních mechanismů a pracuje i přesto s daty jako např. uživatelská jména a hesla. (Gupta, 2017)

3.4.3 Data

Tato kapitola je zamřena na identifikaci vybraných útoků a hrozeb v rámci IoT. Identifikace proběhne jen z hlediska dat uložených v zařízeních IoT lokálně či v Cloudu u zprostředkovatelů. Pohyby dat a jejich útoky byly vysvětleny v předešlé kapitole.

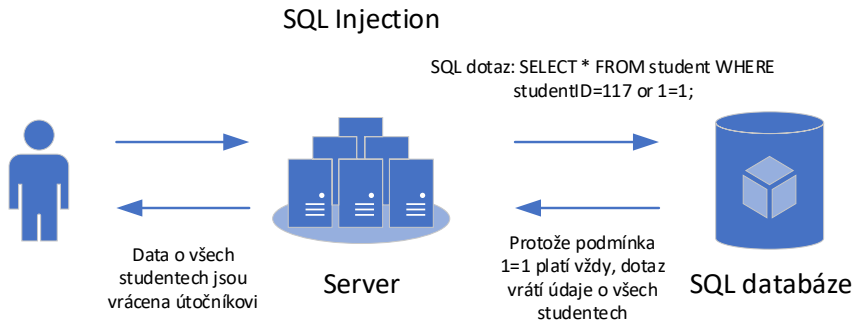
Únik dat – Výsledkem tohoto útoku je únik dat. Jestliže se jedná o zařízení, které lokálně ukládá data na zařízení, je riziko dalšího útoku pravděpodobnější. Je to z důvodu nedostatečné bezpečnosti a správy klíče v případě, že se jedná o zařízení, pracující pod mezinárodní sítí v různých geografických podmínkách.

Útok na účty – Krádež účtu je nejpravděpodobněji zapříčiněna slabým heslem či nedostatečně relevantním identifikačním mechanismem. Útočník může ohrozit, manipulovat a přesměrovat citlivá data.

Správa nepotřebných dat – tím, že je možné zařízení obnovit do původního stavu, je možnost znovu uvedení tohoto zařízení do provozu a získání jeho dat. Za tento typ útoku může nedostatečná správa a vyřazených zařízení.

Manipulace s daty – nelegální manipulace s daty lze dosáhnout dvěma způsoby: za prvé využíváním různých zranitelných míst v rozhraní, jako je tzv. SQL Injection, což je útok na

databázový systém anebo skriptování mezi stránkami. Za druhé je to využití slabých bezpečnostních mechanismů, jako jsou slabá hesla. (Gupta, 2017) Příklad útoku pomocí SQL Injection je na obrázku č.18.



Obrázek 18 - Příklad SQL Injection
Zdroj: https://www.cloudflare.com/img/learning/security/threats/sql-injection-attack/sql-injection-infographic.png

Tzv. Brute force – útok používající automatizovaný software pro generování obrovského počtu odhadů, které umožňují dekódovat šifrovaný text.

3.4.4 Software

V IoT systémech je důležité oddělovat pojmy jako je bezpečnost IoT a bezpečnost dat. V některých případech se totiž může útočník dostat k přístupu zařízení, ale nijak nemůže ovlivnit data, která jsou šifrována. V následujících odstavcích jsou zanalyzovány možné útoky, které se týkají přímo aplikací v IoT zařízení. Aplikace v IoT můžeme rozlišit do 3 kategorií, podle úrovně aplikace. První úrovní je firmware, další operační systém a jako poslední samotné aplikace.

Vývoj IoT aplikací se realizuje v rámci webového rozhraní a převážně se jedná o aplikace, které málokdy fungují jako samostatná jednotka. Dnešní aplikace jsou realizovány způsoby, Kdy je každá aplikace propojená s aplikací jinou a každá z nich hraje klíčovou roli v celku. Tato zranitelnost většinou vede k útokům, které jsou vedeny na 2 a 4 vrstvu architektury (viz úvodní kapitola). Následující útoky zaměřeny zejména na webové rozhraní.

Využití nesprávné konfigurace – jak bylo zmíněno v úvodu, aplikace jsou většinou realizovány jako soubor aplikací, na sebe závisejících. Toto může být problém pro řešení, které slouží jako podpora některých komponent (např. databáze, server atp.). Jejich nesprávná konfigurace totiž může vést k bezpečnostním problémům v aplikaci.

Infikování škodlivého kódu – tento typ útoku je založený na vložení škodlivého kódu do originálního celku. Škodlivý kód poté slouží jako prostředek k odcizení či úpravě osobních dat a také k zisku přístupových údajů na pozdější manipulaci se zařízením. Příkladem takového kódu je např. SQL Injection, což je útok založený na infikování databáze a úpravě dat v ní.

Malware – představuje útok, založený na stejném principu jako předešlá varianta. Nicméně se zde používá přímo vytvořeného softwaru – Malwaru. Je to software zahrnující počítačové viry, trojské koně a různé špehovací softwary.

V případě posunu na další aplikační úroveň směrem dolů se jedná o samotný operační systém. Nicméně i na samotný OS může být zaútočeno několika odlišnými způsoby

Tzv. **Phishing útok** – jedná se o největší bezpečnostní výzvu pro uživatele či společnosti, které vyvíjejí software. Pod tímto útokem stojí totiž zcizení osobních údajů za použití podvodných emailů, hackování smartphonů nebo sociálních medií.

Viry, červy a trojské koně – tyto tři skupiny pojmů se řadí mezi software, které využívají slabin operačních systémů a napadají objekty. Pomocí dalších metod poté ohrožují bezpečnost objektů v IoT.

Brute-force útoky – útok, který je zmíněn v kategorii Dat. Funguje na stejném principu jako v případě aplikací.

Poslední a zároveň nejnižší úrovní mezi aplikacemi je firmware. Firmware je systém, který se stará o základní funkci zařízení na úrovni funkčnosti komponent. To představuje rozdíl oproti operačnímu systému, s nímž je často zaměňován. Tento firmware je pro fungování a bezpečnost IoT naprosto zásadní, protože jeho nestandardní úprava dokáže ovlivnit následnou funkčnost zařízení.

V případě firmwaru se jedná o velmi podobné útoky jako tomu je u aplikací a operačního systému. Jsou to útoky jako malware, úprava kódu apod. Jediným odlišným útokem je tzv. Reverzní inženýrství.

Reverzní inženýrství – je forma útoku, kdy se útočník snaží porozumět tomu, jak daný systém funguje. Na základě tohoto zjištění se snaží sestrojit jemu podobný systém a následně toho využít ve svůj prospěch.

V této kapitole proběhla analýza rizik IoT. Tato analýza byla provedena za použití obecného high-level chématu IoT a pozdějšího rozepsání na nižší úrovně. Definování rizik a pojmenování útoků bylo založeno na základě předešlýchh kapitol o bezpečnosti. Tato kapitola slouží pro následující vytvoření pravidel k bezpečnému použití IoT. (Childs, 2017)

4 Vytvoření pravidel pro použití internetu věcí

První kapitola se zabývala základní seznámením s IoT a jeho technologiemi. V další kapitole byla zmíněna základní problematika bezpečnosti a následovala kapitola celkové analýzy IoT, v které se spojily základní teorie bezpečnosti s funkcemi IoT, přičemž výsledkem kapitoly bylo definování rizik a způsobů útoků. Tato kapitola je praktickou částí diplomové práce a je to výsledek, ke kterému práce od začátku směřuje. Úvod této kapitoly obsahuje ohodnocení pravidel pro případně rozhodování o důležitosti implementace. Následně pokračuje pravidly pro využití IoT výrobcem, uživatelem a jsou zde taktéž definovány okruhy, na které by se měl zaměřit mobilní operátor.

4.1 Ohodnocení pravidel

Před vyjmenováním pravidel je nejprve nutné definovat jejich důležitost. Pro výrobce či pro uživatele je to způsob, jakým lze odlišit různě náročná pravidla na implementaci a jejich případné vynechání.Pravidla jsou rozdělena do 3 základních skupin: s vysokou, střední a nízkou prioritou.

Pravidla s vysokou prioritou jsou typem doporučení, která zasahují do architektury zařízení a bezpečí uživatele. Soubor doporučení s vysokou prioritou by měl být proveden pouze, pokud to vyžaduje samotná architektura zařízení. Např. ne všechny zařízení vyžadují odolný kryt vůči poškození.

Soubor doporučení se střední prioritou zahrnuje soubor doporučení, která jsou relevantní v závislosti na volbě návrhu technologie zařízení. Doporučení týkající se operačních systémů nejsou relevantní v případě, že se na zařízení operační systém nenachází.

Nízkou prioritou jsou označeny doporučení, která se vztahují na rizika, která jsou extrémně nákladná na zabezpečení, jsou nejméně pravděpodobná a nedokáží omezit funkčnost zařízení.

Znázornění pravidel je zobrazeno na konci každého pravidla. V příloze A a B jsou priority zařazeny také. V obou případech pod písmeny V, S a N (Vysoká, střední a nízká priorita).

4.2 Výrobce IoT

První skupinou, které se tato kapitola věnuje, jsou výrobci. Obecně lze říci, že výrobci mohou zaujmout zpravidla dvě postavení vůči IoT. Prvním postoj zaujímá firma vyrábějící HW pro IoT, která spolupracuje s některou z platforem uvedených v první kapitole. Anebo ke svému vyrobenému **HW** vytváří také IoT **SW**. Pravidla jsou brána jako celek pro obě kategorie, každopádně jsou situována jako oblast, které by se výrobce měl věnovat. Následně jsou vypsaná pravidla.

4.2.1 Klasifikace dat

Pojem data je velmi široký a může obsahovat spoustu údajů, např. data o lidech, funkční data, osobní data. Citlivost těchto dat závisí na stupni ochrany, který by měl výrobce implementovat před neoprávněným zobrazením. Proto je v první řadě potřeba definovat „schéma klasifikace dat“. Toto schéma definuje typ dat v zařízení a úroveň citlivosti pro každou kategorii. Může tak být aplikována bezpečnost v závislosti na povaze dat. Tato klasifikace také pomůže zajistit správnost z právního hlediska. Pravidla tedy jsou:

1. Definovat a zdokumentovat typ dat – N
2. Ohodnotit každý typ dat dle jejich způsobu použití – N
3. Bezpečnostní mechanismy podle ohodnocení dat – V

4.2.2 Fyzická bezpečnost

Jak bylo zmíněno v předešlých kapitolách, IoT zařízení jsou často na neobvyklých místech, která mohou být snadno přístupná. Mohou tak být vystavena vnějším útokům, jako například fyzickému poškození či přímé manipulaci se zařízením. Zařízení by tak měla být chráněna proti fyzickému přístupu a zameznit možnosti připojení k danému zařízení. Z těchto podmínek poté vyplývají následující pravidla:

1. Součástí finálního zařízení by neměla být rozhraní pro účel správy tohoto zařízení, popř. zakázáné nebo fyzicky nepřístupné. - V

2. Všechny porty, které sloužily pro testování, by na produkčních zařízení měly být vypnuty či odstraněny. - V
3. Pokud zařízení obsahuje administrační port je potřeba zajistit silnou ověřovací ochranu. - V
4. Zajištění obvodů v zařízení proti fyzické manipulaci. - V
5. Zajištění bezpečného ochranného pouzdra. - V
6. Pouzdro by mělo obsahovat ochranné známky vůči nedovolené manipulaci. - N

4.2.3 Zabezpečený start zařízení

Start zařízení je kritickým procesem, který zajišťuje následnou integritu a funkčnost. Při startu probíhá několik etap zavádění komponent do běhu a je potřeba na tento proces dbát zvýšenou pozornost. Pravidla jsou následující:

1. Rozdělit start zařízení do více etap – V
2. Každou etapu před inicializací zkontrolovat – V
3. Každá etapa by měla před zavedením komponenty zkontrolovat její HW parametry – V
4. Ověření zdrojových kódů při startu zařízení – V
5. Jestliže dojde k selhání, zajistit, aby selhání nevedlo k neoprávněnému přístupu k zařízení – V

4.2.4 Zabezpečný operační systém

Z předešlé kapitoly je známo, že k narušení operačního systému vede nespočet cest. Elementárním pravidlem operačního systému je fakt, že by OS měl vždy obsahovat nejnovější verzi bezpečnostních aktualizací či softwaru jako takového. Nicméně existují další důležitá pravidla:

1. Operační systém by měl obsahovat pouze ty komponenty, které jsou nezbytně nutné pro jeho funkci. - S
2. Služby, protokoly a porty, které nejsou používány by měly být zakázány. - S
3. Zajištění bezpečného startu operačního systému. - S

4. Nastavení odpovídajícího oprávnění pro dané zařízení/aplikace/uživatele. - V
5. Ujištění, že všechny soubory a adresáře mají minimální přístupová práva. - V
6. Implementace šifrovaného souborového systému. - V

4.2.5 Aplikační prostředí

Bez ohledu na to, zda je použit vlastně vyvíjený software či software třetí strany, musí být dodrženy některé postupy při navrhování těchto typů softwarů. Při vývoji musí být brána v potaz bezpečnost už od samotného začátku. Pro tuto kategorii existují pravidla:

1. Zdokumentování návrhu zabezpečení aplikací. - N
2. Aplikace, které jsou spuštěny musí být provozovány na nejnižší možné úrovni z hlediska oprávnění. Spuštění aplikací s oprávněním jako administrator či root je nepřípustné. - V
3. Aplikace a jejich procesy by měly být odděleny od sebe. Využití principu, kdy každá aplikace je spuštěná ve svém vlastním „tzv. sandboxu“. - V
4. Při vývoji užití bezpečnostních technik návrhu a kódování. Např. oveřené vstupy dat před zpracováním atp. - V
5. Otestování toho, zda jsou vyřešeny veškeré chyby a zároveň jsou zobrazeny pouze ta data, která mají být zobrazena. - S
6. Odstranění výchozích účtů a hesel, které výrobce využíval pro testování. -V
7. Zajištění kroků v případě ztráty internetového připojení. Např. uložení posledních dat do paměti či samotné zachování běhu aplikace. - S

4.2.6 Správa pověření

Proces pověření je postup, který prokazuje totožnosti subjektů v systému IoT. Proces má mnoho podob a slouží k řízení přístupu k datům či ke komunikaci. Získání poveření je nejjednoduší postup, jak dojít k citlivým datům, proto má tato tento proces zvláštní pravidla:

1. Zařízení by mělo být jednoznačně identifikováno pomocí hardwaru. – V
2. Ukládání šifrovacích klíčů na k tomu určený modul, který je také náležitě zabezpečen. – V

3. Implementace 2 ověřování pro přístup k citlivým datům. – V
4. Správná technika volby hesel. – V
5. Každé heslo musí být kryptováno. – V
6. Zajištění spolehlivého a důvěryhodného zdroje času, neboť některé metody ověřování využívají čas jako součást ověření. Např. digitální certifikáty – V
7. V případě digitálních certifikátů musí být správně definována jejich životnost, musí být provedena následná aktualizace a také jednoznačná identifikace. – V
8. V případě „továrního nastavení“ musí být hesla a citlivé údaje trvale odstraněna. – V

4.2.7 Šifrování

Použitím šifrování v dnešní době je absolutní nutnost. Všechna data, která jsou přiřazena objektům, musí být náležitě zašifrována. Zajistí se tím soukromí a také právní náležitosti platné pro danou legislativu. Následující pravidla pro kategorii šifrování:

1. Aplikace odpovídající úrovně šifrování pro odpovídající typ dat. – V
2. Použití standardizovaných šifrovacích metod. – V
3. V případě standardizovaných šifrovacích metod používat vždy jejich nejnovější verzi. – S
4. Implementace zvlášť oddělené paměti pro šifrovací klíče. – V
5. Vyhnout se použití nezabezpečených protokolu jako FTP, Telnet. – V

4.2.8 Síťová připojení

Z předešlých kapitol je známo, že zařízení komunikuje se světem pomocí síťových připojení. Proto je nezbytné tyto body chránit a omezit možné cesty k těmto bodům na minimum.

1. Aktivace pouze těch síťových rozhraní, která jsou v danou chvíli vyžadována. – S
2. Spouštění pouze těch služeb, které jsou v danou chvíli vyžadována. – S
3. Zakázání síťových portů, která nejsou používána. – S
4. Vždy používat zabezpečené protkoly jako HTTPS. – V
5. Nikdy nepřenášet citlivá data přes nezabezpečený protokol. – V
6. Ověření každého připojení, zda pochází z ověřeného zdroje. – V

7. Před odesláním citlivých dat, ověřit příjemce dat. – V

4.2.9 Zabezpečení softwarových aktualizací

Zařízení IoT obsahuje několik typů programového vybavení. Je to samotný operační systém, aplikace anebo také firmware. Aktualizace těchto softwarů poskytuje prostředky k opravě stávajících chyb v zabezpečení či chyb ve funkčnosti zařízení. V ideálním případě jsou zařízení schopna aktualizací tzv. na dálku, kdy se aktualizace stahují přes internet a instalace probíhá automaticky. Alternativní způsob je publikování softwaru prodejcem a manuální aktualizace uživatelem. Uživatele by tyto aktualizace měly získávát pouze z ověřeného zdroje, jako je například oficiální stránka výrobce. Pro výrobce to pak je několik pravidel, které by měl dodržet:

1. Zašifrování aktualizačního balíčku k zabránění tzv. reverzního inženýsrtví. – S
2. Aktualizační proces musí být před instalací ověřen, zda splňuje podmínky integrity a pravosti. – V
3. Zajištění, aby instalační balíček nemohl být změněn či nahrazen mezi procesem validace a instalace. – V
4. Implementovat mechanismus, kdy se v případě neúspěšné instalace vrátí původní nstavení v známém funčkním stavu. – V

4.2.10 Zásady vydávání softwarových aktualizací

Výrobci zařízení a systémů IoT musí mít zásady, které se týkají aktualizace softwaru jejich zařízení. Mezi tyto zásady patří:

1. Správa všech zařízení po celou dobu jejich životnosti:
    a. Aktivní správa verze jejich softwaru. – S
    b. Proces plánování a vydávání kritických aktualizací. – V
    c. Identifikace zařízeních, která jsou ne-opravitelná či ne-aktualizovatelná a jsou známé jejich zranitelnosti. – S

2. Publikovaný proces řízení softwaru. Proces, kdy výrobci informují uživatele o bezpečnostních rizikách a jiných problémech, které jsou spojené s daným zařízením. – V
3. Jasně definované mechanismy pro aktualizaci softwaru. – S

4.2.11 Vytváření záznamů

Vytváření záznamů je nezbytným procesem pro řešení poruch a zabezpeční. Proto musí být tento proces spolehlivý, přístupný a hlavně důvěrný. Veškerá aktivita v zařízení je tak monitorována a pravidelné analyzována. Pro tento důležitý proces existuje několik pravidel:

1. Zajištění, aby zaznamenaná data byla v souladu s platnými právními předpisy na ochranu dat. – S
2. Proces tvoření záznámů by měla být funkce oddělená od všech ostatních. – N
3. Ukládádní výsledků by mělo probíhat taktéž odděleně jako je tomu u pravidla č.2. – N
4. Nastavení maximální velikosti těchto záznamů. – N
5. Pokud je kapacita záznamů omezena, zaznamenávat pouze neočekávané procesy. – N
6. Omezení přístupových práv tohoto procesu na minimum potřebné k fungování. – N
7. Ujištění, že přenos dat probíhá po zabezpečeném kanále. – S
8. Synchronizace s přesným časovým údajem. – S
9. Hesla a citlivé údaje by neměla být nikdy zobrazena v těchto záznamech. – V

4.3 Uživatel IoT

V případě uživatele IoT jsou pravidla značně stručnější. Je to kvůli tomu, že uživatel jako takový může zařízení a jeho bezpečnost ovlivnit pouze jeho proaktivitou, nikoliv zásahem do něj. Formu pravidel pro použití zařízení IoT vydává i samotný výrobce. Je to soubor pravidel, kterými se daný výrobce určitým způsobem chrání proti důsledkům, které by mohla způsobit zařízení, jestliže se s nimi manipuleje nevhodným způsobem. Jestliže daný výrobce

vydá pravidla k použití a uživatel si nevhodným použitím způsobí újmu, výrobce se tak odvolává na zmíněná pravidla a nenese za škody žádnou odpovědnost.

Z důsledku rozšířenosti IoT, jsou pravidla pojata velmi obecně. Je to proto, aby platila na většinu zařízení, která jsou na trhu dostupná. V následujícím odstavci jsou uvedená pravidla, které platí pro IoT. Pravidla jsou obecným návrhem a je možné je použít jako inspirace pro výrobce těchto zařízení.

Pravidla pro uživatele:

1. Mobilní zařízení, které spravuje danou sít IoT je třeba chránit před neoprávněném zneužití, kráděží či ztrátou. Brát v úvahu obecné zásady pro bezpečnost při používání internetu. V případě nutnosti svoje mobilní zařízení chránit určitou softwarovou ochranou, a především pravidelně aktualizovat software. - S
2. Neupravovat HW ani SW zařízení IoT. - V
3. Neupravovat mobilní zařízení, které spravuje síť IoT. Úpravy jako mobilního zařízení jako např. „root“ u zařízení se systémy Android či jailbreak u zařízení od firmy Apple. - V
4. Neinstalovat aplikace třetích stran, které nejsou ověřené a neobsahují digitální podpis. - V
5. V případě mobilních zařízení stahování dodatečného softwaru pouze z oficiálních míst pro to určené (např. Apple App Store či Google Play Store). - V
6. Dodatečně zakoupená IoT zařízení musejí být zpětně kompatibilní se sítí, která již existuje a také zpětně kompatibilní se zařízením, které toto zařízení spravuje. V nejlepším případě by zakoupená zařízení měla obsahovat štítky podobné certifikaci Apple Homekit na obrázku č.6. - N
7. V případě bezpečnostních hlášení, respektovovat je a řešit případnou poruchu s výrobcem. Nikoliv svépomocí. - N
8. Veškerá zařízení IoT a zařízení, která spravují síť IoT je třeba vždy aktualizovat, pokud to výrobce umožňuje. - S
9. Nikomu nesdělovat své osobní a přihlašovací údaje. - V
10. Dbát na bezpečnostní zásady při vytváření přihlašovacích údajů a především hesel. - V

11. V případě podezření, že se zařízení IoT či samotný uživatel stal středem zájmu útočníka, je třeba podnikat kroky, které vedou k okamžité zastavení činnosti. Především ukončení spojení s internetem, fyzické zkontrolování zařízení a následné kontaktování výrobce. - V

4.4 Mobilní operátor

Dnešní mobilní sítě podporují různé síťové služby jako je: VoIP, HD přehrávání videií, internetové televize, elektronické platby či zprostředkovatel cloudu. Proto je potřeba implementace několik bezpečnostních mechanismů. V případě mobilní sítě je zde několik skupin, které souvisí právě s IoT. Tyto skupiny jsou rozděleny podle typu použité technologie.

První skupinou jsou GSM/GPRS sítě. Tyto sítě jsou také známy jako sítě druhé generace a mobilní operátor, který podporuje tyto sítě by měl zahrnout ve své síti prinicipy jako:

1. Ochrana spojení mezi End-to-end zařízeními pomocí 128bitovou šifrou a vyvarování se jakkékoliv nešifrované komunikace.
2. Implementace autentifikačních alogritmů

V sítích druhé generace není síť ověřená koncovým zařízením, pouze zařízení je ověřeno sítí, což může být jako potenciální riziko pro uživatele, který se připojí pod falešnou síť druhé generace.

Druhou skupinou je síť třetí generace, známá také pod zkratkou UMTS. Tato generace sítě umožňuje vzájemné ověřování, kdy zařízení není pouze ověřeno sítí, ale i síť je ověřena zařízením. Sítě, které podporují UMTS by měla obsahovat výše zmíněný autentifikační alogirtmus MILENAGE a také algoritmus pro generování klíčů.

Další ve skupině známých sítí je poslední generace s názvem 4G, nebo také tzv. LTE. Operátoři, kteří poskytují tento typ sítě, musí podporovat výše zmíněné ověřovací algoritmy MILENAGE a také typ šifrování, které se nazývá LTE EEA1, EEA2 nebo EEA3.(Childs, 2017)

Další skupinou je méně známá technologie pro zařízení s nízkou spotřebou. GSMA tvrdí, že operátor musí zajistit takovou úroveň zabezpečení, která je třeba v závislosti na nákladech, životnosti baterií v zařízeních anebo pokrytí sítě. Některé důležité prvky bezpečnosti jsou uvedeny v následujícím seznamu:

1. Šířka pásma, včetně stanovení maximálního stahování a nahrávání.
2. Denní propustnost dat
3. Autentizace – zabezpečené připojení k síti vyžaduje, aby se různé strany navzájem autentizovaly.
4. Důvěrnost dat – zajištění důvěrnosti šifrováním, které se obvykle používá k tomu, aby byla data v bezpečí před potenciálním útočníkem. Bezpečnost následně může být navýšena zavedením bezpečnostních mechanismů na aplikační vrstvě v rámci end-to-end zařízení.
5. Poskytování klíčů – Kryptografické techniky pro autentizaci, důvěrnost a integritu závisí na kryptografických klíčích, které jsou sdíleny mezi stranami.
6. Ověřená zařízení – na některých trzích je vyžadována certifikace při koupi zařízení s datovou technologií, než je samotný produkt prodáván.
7. V případě protokolu IP zde vzniká možnost „otevření se“ internetu a možnost potenciálního útoku na dané zařízení. Z tohoto důvodu musejí být zváženy bezpečnostní postupy a prvky pro protokol IP ze strany operátora.

Mobilní operátoři mohou IoT službám poskytovat mezinárodní mobilní připjení, což je také další kategorie v oblasti bezpečnosti mobilních operátorů. Roamingové sítě mohou být ohroženy narušením bezpečnosti kvůli jejich relativní otevřenosti, která plyne ze vzájemného propojení mezi domací a cizí sítí. Toto téma je zvláště důležité pro služby IoT, které používají svá zařízení v roamingových sítích. Podíl těchto zařízení je značný a existuje k tomu několik důvodů. Prvním důvodem je, že mnoho zařížení se vyrábí na jednom místě, ale jejich distribuce probíhá globálně. A za druhé, je v některých případech totiž mnohem výhodnější použití roamingu než místní sítě.

Bezpečnostní funkce, které je třeba implementovat, aby odpovídajícím způsobem chránily prostředky a služby IoT jsou specifické pro každou službu. Proto zůstává odpovědědnost především na výrobci služeb IoT. V některých případech mobilní operátoři a výrobci služeb

úzce spolupracují na zabezpeční v případě vývoje zařízení IoT a předcházejí tomu smluvní domluvy. V jiných případech mobilní operátor nabízí výrobci IoT některé bezpečnostní služby, které mohou poskytnou klíčovou roli při zabezpečení řešení IoT. Největším bezpečnostním mechanismem, kterým může operátor zajistit bezpečnost pro daného výrobce IoT, je vytvoření samostatné sítě. Do sítě má poté přístup pouze povolená zařízení výrobcem a výrobce tak předchází potenciálním útočníkům ze strany internetu.

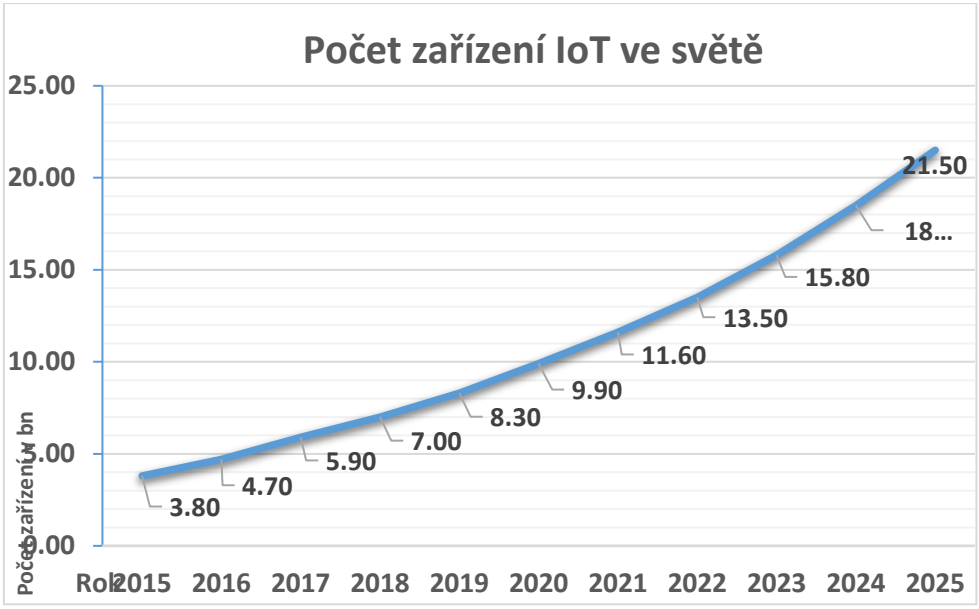
5 Vyhodnocení praktického přínosu v oblasti bezpečnosti internetu věcí

Předchozí kapitola č. 4 byla samotnou praktickou částí diplomové práce. Byla systematicky rozdělena do tří elementárních částí: Výrobci IoT, Uživatel IoT a nakonec samotný operátor. Z pohledu bezpečnosti je tím nejdůležitějším aspektem samotný výrobce, protože vždy záleží přímo na něm, jaké navrhne zařízení a jak toto zařízení bude chráněno z hlediska bezpečnosti. A z toho důvodu byla sekce o bezpečnosti rozebrána v rámci práce nejrozsáhleji, kdy byly samotné bezpečnostní aspekty rozebrány do detailů. Samotná zkrácená verze bezpečnostního manuálu je umístěná v příloze B.

Další rolí ve schématu je samotný uživatel. Kapitola pravidel o uživateli je zdaleka nejstručnější, neboť uživatel jako takový může málo kdy ovlivnit bezpečnost zařízení, které kupuje. Nutno říci, že se to od něj ani neočekává. Uživatel hraje v tomto případě pouze proaktivní roli, a tak je sepsán i bezpečnostní manuál. Zkrácená verze bezpečnostního manuálu pro uživatele je přiložena v příloze A

Poslední kategorií je mobilní operátor, který hraje podstatnou roli ve smyslu funkčnosti IoT, nicméně v pohledu bezpečnosti je to role zdaleka nejmenší. Nízkou roli operátorům přiřazují především samotní výrobci. A z toho důvodu, že výrobců, kteří ochotně spolupracují s operátory, je velmi malé množství. Vyplývá to z uplatnění SIM karet v daném zařízení, některé zařízení se totiž spokojí s technologií Wi-Fi a pro výrobce tak odpadá nutnost řešení mobilních dat. Největším zástupcem výrobců IoT, ve kterých se používá SIM karta je automobilový průmysl a slovní spojení Connected Car. V tomto odětví probíhá přímé propojení automobilu s internetem za užití simkarty.

Podle deníku Forbes bude počet zařízení IoT (Internet of Things), která jsou ve zdravotnictví v roce 2020, atakovat hranici $0.117 Bilionu. (Mccue, 2015) Následující obrázek č. 19 ukazuje rozšíření IoT zařízení a jejich předpověd do roku 2025. Je patrné, že tendence paradigmatu IoT je rostoucí. S tímto trendem lze zcela jistě říci, že poroste počet potenciálních cílů i počet útoků.



Obrázek 19 - Počet zařízení do roku 2025
Zdroj: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

Růst IoT trhu také znamená růst potenciálních možností pro firmy a osoby, které se zajímají o tento obor. Jaká je tedy potom přidaná hodnota této diplomové práce, resp. Pravidel pro použití IoT?

Přidaná hodnota má několik stran a každý může považovat za přidanou hodnotu něco jiného. Obecně lze říci, že je to užitek, který přináší zakoupené zařízení IoT uživateli. V případě uživatele přidanou hodnotu lze definovat jako užitek, který plyne díky podstoupení kroků ke zlepšení své vlastní bezpečnosti. V případě výrobce je to užitek především v podobě zisku z prodaných zařízení IoT, každopádně tento zisk může plynout i například z pověsti bezpečného výrobce s bezpečnými IoT zařízeními. S tím by zcela jistě narostl zájem uživatelů o nabízený produkt tím pádem dochází k nárustu počtu tržeb a užitku výrobce IoT.

Odpovědí na praktický přínos této diplomové práce je podoba proaktivní ochrany uživatele. A to především z pohledu daného uživatele, který by měl udělat potřebné kroky pro zabezpečení svého zařízení.

Z pohledu výrobce je výstupem této práce seznam pravidel, která je možné využít v rámci zlepšení bezpečnosti v problematice IoT. Tato pravidla mohou být brána taktéž jako podpůrný prostředek k bezpečnému vývoji, návhru a následnému provozu IoT zařízení a jeho sítě.

Společným výstupem je možnost aplikace velké většiny výše zmíněných bodů do všech aspektů IoT. Autor práce se snažil veškeré body zobecnit a zestručnit tak, aby jejich následná aplikace byla co možná nejjednodušší. Finální výstupem práce je tisknutelná verze manuálu v přílohách A a B, které slouží v tiskové podobě jako kontrolní seznam splněných kritérií.

.

Závěr

Cílem této diplomové práce bylo vytvoření pravidel pro bezpečné použití Internet of Things. Teoretická část si kladla za cíl seznámit čtenáře s teoretickým pozadím problematiky Internet of Things a také základními znalostmi jeho bezpečnosti. Úkolem v praktické části bylo následné vytvoření pravidel pro bezpečné využití IoT jak z pohledu výrobce, tak z pohledu uživatele.

V první části je popsána současná situace v odvětví IoT. Je zde jasně vymezen pojem IoT a jeho výhody. Dále je stručně popsána jeho architektura spolu s popisem jednotlivých vrstev. Právě zmíněná architektura a rozpis do funkčních vrstev hraje v této práci podstatnou roli vedoucí k porozumnění praktické části diplomové práce. Závěr kapitoly podtrhují reálné příklady užití IoT.

Další část, se nazývá Zhodnocení a srovnání bezpečnostních norem platných pro Internet věcí. Tato část seznamuje čtenáře s obecnou bezpečností v IoT a vymezuje její důležité aspekty. Následně popisuje existující bezpečnostní souhrn platným pro IoT, kterému se věnuje externí firma. Tato kapitola tak uzavírá teoretickou část diplomové práce, která měla za úkol shrnout a popsat IoT jako celek spolu s jeho bezpečností.

Třetí část diplmové práce, která nese názevAnalýza rizik internetu věcí je kapitola spojující informace z předešlých kapitol. Výsledkem této analýzy je poté high-level zobrazení jednotlivých účastníků komunikace v IoT a jejich následné spojení v celkovém řešení. Na závěr kapitoly jsou ze schémat odvozená rizika. Definování rizik je podstatnou částí této kapitoly, protože při řešení bezpečnosti je znalost rizik kritická. Rizika jsou popsána jako formy útoku kategorizovány podle rovin, ve kterých je útok uskutečňován.

Předposlední část a praktický přínos této diplomové práce je vytvoření pravidel pro použití internetu věcí. Tuto kapitolu lze chápat jako soubor pravidel, které slouží k bezpečnému navrhování a používání IoT. Celá kapitola je pojmuta do tří skupin, kde první skupina řeší pravidla pro výrobce IoT, což je soubor pravidel, který by měl výrobce dodržet, jestliže chce vyrábět bezpečné zařízení IoT. Druhou skupinou je samotný uživatel IoT. Pravidla, která jsou definována pro uživatele IoT jsou souborem pravidel, který velmi obecně popisuje práci

s IoT. Jako poslední skupina je v této kapitole role mobilního operátora. Tato role je v práci popsána jako zprostředkovatel internetu a hraje tak klíčovou část v komunikaci. Nicméně pravidla pro mobilního operátora jsou uvedena velmi obecně, důvodem je neochota operátorů sdělovat své know-how.

Závěrečnou kapitolou je pak nastínění praktického přínosu pravidel a určitý pohled na ekonomické zhodnocení. Dále podtrhuje, že tato diplomová práce neslouží pro výrobce, uživatele a mobilní operátory jako manuál, kterým lze perfektně zabezpečit zařízení IoT. Práce slouží jako úvod problematiky IoT a je velmi vhodné ji použít jako podklad pro rozsáhlou práci v daném odvětví.

Seznam použité literatury

BURIAN, Pavel, 2014. *Internet inteligentních aktivit*. Praha: Grada. Průvodce (Grada). ISBN 978-80-247-5137-5.

BUNZ, Mercedes a Graham MEIKLE, 2017. The Internet of things. Malden, MA, USA: PolityISBN 978-1509517459.

GUPTA, Aditya. 2017 IoT Hackers Handbook: An Ultimate Guide to Hacking the Internet of Things and Learning IoT Security. CreateSpace Independent Publishing Platform. Průvodce (Grada). ISBN 1974590127.

HU, Fei a Graham MEIKLE. 2016. Security and privacy in internet of things (IoTs): models, algorithms, and implementations. Boca Raton: Polity. ISBN 978-1498723183.

TRIPATHY, B. K a J. ANURADHA. 2018. Internet of things (IoT): technologies, applications, challenges and solutions. Boca Raton: Centre national des Lettres. ISBN 978-1138035003.

CHILDS, Rob. 2017 IoT Security Guidelines for IoT Service Ecosystems [online]. 2017(CLP.12) [cit. 2019-03-16]. Dostupné z: https://www.gsma.com/iot/wp-content/uploads/2019/01/CLP.12-v2.0.pdf

CHILDS, Rob. 2017. IoT Security Guidelines for Endpoint Ecosystems [online]. 2017(CLP.13) [cit. 2019-03-16]. Dostupné z: https://www.gsma.com/iot/wp-content/uploads/2019/01/CLP.13-v2.0.pdf

CHILDS, Rob. 2017. IoT Security Guidelines for Network Operators [online]. 2017(CLP.14) [cit. 2019-03-16]. Dostupné z: https://www.gsma.com/iot/wp-content/uploads/2019/01/CLP.14-v2.0.pdf

ASIM, Makkad. 2017. *A Survey on Application Layer Protocols for Internet of Things (IoT)* [online]. Institute of Technology, Nirma University, India. [cit. 2019-03-16]. ISSN 976-5697. Dostupné z: http://www.ijarcs.info/index.php/Ijarcs/article/view/3143/3119

MILLER, Lawrence. 2016. *IoT Security For Dummies*® [online]. West Sussex: John Wiley, 2016 [cit. 2019-03-16]. ISBN 978-1-119-21118-1. Dostupné z: https://www.insidesecure.com/index.php/cn/Media/Files/IoT-for-dummies

BACHMANN, Michael, 2014. Passwords are Dead: Alternative Authentication Methods. *2014 IEEE Joint Intelligence and Security Informatics Conference*[online]. IEEE,

2014, 322-322 [cit. 2019-04-02]. DOI: 10.1109/JISIC.2014.67. ISBN 978-1-4799-6364-5. Dostupné z: http://ieeexplore.ieee.org/document/6975605/

MCCUE, TJ. 2015. *64,471 viewsApr 22, , 05:25pm $117 Billion Market For Internet of Things In Healthcare By 2020* [online]. [cit. 2019-03-16]. Dostupné z: https://www.forbes.com/sites/tjmccue/2015/04/22/117-billion-market-for-internet-of-things-in-healthcare-by-2020/#5d63b16269d9

SINGH, Sachchidanand a Nirmala SINGH. 2015 *Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce* [online]. IEEE [cit. 2019-03-17]. DOI: 10.1109/ICGCIoT.2015.7380718. ISBN 978-1-4673-7910-6. Dostupné z: http://ieeexplore.ieee.org/document/7380718/

EVANS, Dave. 2011. *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*[online]. [cit. 2019-03-17]. Dostupné z: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

DORSEMAINE, Bruno, Jean-Philippe GAULIER, Jean-Philippe WARY, Nizar KHEIR a Pascal URIEN, 2015. Internet of Things: A Definition. *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies* [online]. IEEE, 2015, 72-77 [cit. 2019-04-02]. DOI: 10.1109/NGMAST.2015.71. ISBN 978-1-4799-8660-6. Dostupné z: http://ieeexplore.ieee.org/document/7373221/

MADAKAM, Somayya, R. RAMASWAMY, Siddharth TRIPATHI, Nizar KHEIR a Pascal URIEN, 2015. Internet of Things (IoT): A Literature Review. In: *Journal of Computer and Communications* [online]. IEEE, 2015, 03(05), s. 164-173 [cit. 2019-03-17]. DOI: 10.4236/jcc.2015.35021. ISBN 978-1-4799-8660-6. ISSN 2327-5219. Dostupné z: http://www.scirp.org/journal/doi.aspx?DOI=10.4236/jcc.2015.35021

BERNERS-LEE, Tim. 2016. Internet Live Stats. *World Wide Web Foundation* [online]. [cit. 2019-03-17]. Dostupné z: http://www.internetlivestats.com/internet-users/

ROGERS, Bruce. 2014. *Apple and Google Dominate 'Internet of Things' Influence with Home Automation Efforts* [online]. [cit. 2019-03-17]. Dostupné z: https://www.forbes.com/sites/brucerogers/2014/07/08/apple-and-google-dominate-internet-of-things-influence-with-home-automation-efforts/

CARTER, Jamie. 2015. *Which is the best Internet of Things platform?* [online]. [cit. 2019-03-17]. Dostupné z: https://www.techradar.com/news/world-of-tech/which-is-the-best-internet-of-things-platform-1302416

VELOCCI, Carli. 2016. *Internet Access Is Now A Basic Human Right* [online]. [cit. 2019-03-17]. Dostupné z: https://gizmodo.com/internet-access-is-now-a-basic-human-right-1783081865

GOODIN, DAN. 2016. *Record-breaking DDoS reportedly delivered by >145k hacked cameras* [online]. [cit. 2019-03-17]. Dostupné z: https://arstechnica.com/information-technology/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/

GELLES, David, Hiroko TABUCHI a Matthew DOLAN, 2015. *Complex Car Software Becomes the Weak Spot Under the Hood* [online]. New York Times [cit. 2019-04-02]. Dostupné z: https://www.nytimes.com/2015/09/27/business/complex-car-software-becomes-the-weak-spot-under-the-hood.html

CIHI, Radek. 2017. *Eliminace rizik a hrozeb spojených s připojením vozu k internetu* [online]. Liberec, [cit. 2019-03-17]. Dostupné z: https://stag.tul.cz/StagPortletsJSR168/PagesDispatcherServlet?pp_destElement=%23ssSouboryStudentuDivId_804&pp_locale=cs&pp_reqType=render&pp_portlet=souboryStudentuPagesPortlet&pp_page=souboryStudentuDownloadPage&pp_nameSpace=G224078&soubidno=52136. Bakalářská práce. Technická Univerzita v Liberci.

Anonymní autor. 2019. Historie Internetu. *Co je internet?* [online]. [cit. 2019-03-17]. Dostupné z: http://www.imip.cz/internet-historie/

SANNAPUREDDY, Bhaskara Reddy. 2015 Pros & Cons of Internet Of Things (IOT). *LinkedIn* [online]. [cit. 2019-03-17]. Dostupné z: https://www.linkedin.com/pulse/pros-cons-internet-things-iot-bhaskara-reddy-sannapureddy/

Pathak, P. B. 2016. Internet of things: A look at paradigm shifting. *International Journal of Advanced Research in Computer Science, 7*(2) Retrieved from https://search.proquest.com/docview/1798937086?accountid=17116

Seznam příloh

Příloha A - Bezpečnostní manuál pro výrobce v tiskové podobě 1/2 90
Příloha B - Bezpečnostní manuál pro výrobce v tiskové podobě 2/2..... 91
Příloha C - Bezpečnostní manuál pro uživatele v tiskové podobě 92

Příloha A – Bezpečnostní manuál pro výrobce v tiskové podobě 1/2

Příloha B – Bezpečnostní manuál pro výrobce v tiskové podobě 2/2

Příloha C – Bezpečnostní manuál pro uživatele v tiskové podobě